



A University of Sussex PhD thesis

Available online via Sussex Research Online:

<http://sro.sussex.ac.uk/>

This thesis is protected by copyright which belongs to the author.

This thesis cannot be reproduced or quoted extensively from without first obtaining permission in writing from the Author

The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the Author

When referring to this work, full bibliographic details including the author, title, awarding institution and date of the thesis must be given

Please visit Sussex Research Online for more information and further details



THE DESARGUESIAN PROJECTIVE
PLANE OF ORDER ELEVEN AND
RELATED CODES

Awss Al-ogaidi

Thesis submitted for the Degree of Doctor of
Philosophy in Mathematics

February 2020

Declaration

I hereby declare that this thesis has not been and will not be, submitted in whole or in part to another University for consideration of any other degree.

I also declare that this thesis was composed by myself and that the work contained therein is my own, except where specific reference is made to the work of others.

Awss Al-ogaidi

February 2020

Acknowledgements

I would like to express my sincere gratitude to my supervisor Professor James Hirschfeld who supervised the current research and made many valuable suggestions.

I also thank Dr. Anton Betten for his kind guidance and valuable collaboration and especially for the help in Chapter 5, part of another joint paper in [1] of ours which won the best graduate student paper in the 50th Southern International Conference in Florida Atlantic University, USA, in March 2019.

I am honored to be one of the recipients of a scholarship from the Higher Committee for Education Development in Iraq. Many thanks for their generous support.

We are grateful to Microsoft corporation for giving this project the Microsoft Azure Research Award.

Many thanks and deepest gratitude go to CoDiMa project for supporting the collaborative research visit to meet the GAP team in St.Andrews University. Also, not to forget to thank Dr. Alexander Konovalov and the GAP team for their great support.

My sincere thanks due to all members of my family for their support and encouragement.

Abstract

In a finite projective plane $\text{PG}(2, q)$, a set \mathcal{K} of k points is a (k, n) -arc for $2 \leq n \leq q - 1$ if the following two properties hold:

1. Every line intersects \mathcal{K} in at most n points.
2. There exists a line which intersects \mathcal{K} in exactly n points.

Algebraic curves of degree n give examples of (k, n) -arc; the parameter n is called the degree of the arc. In $\text{PG}(2, q)$, the problem of finding $m_n(2, q)$ and $t_n(2, q)$ (the maximum and the minimum value of k for which a complete (k, n) -arc exists) and the problem of classifying such arcs up to projective equivalence, are crucial problems in finite geometry. One of the important application of these arcs in coding theory are projective codes that cannot be extended to larger codes.

The aim of this project is to classify (k, n) -arcs if possible for $3 \leq n \leq 5$ and to construct large arcs in $\text{PG}(2, 11)$. Algebraic and new combinatorial methods are used to perform the classification and the construction of such arcs with different degrees. Those procedures are implemented using different open-source software packages such as GAP [35] and Orbiter [10].

We were successful in obtaining new isomorphism types of $(k, 5)$ -arcs for $k = 5, \dots, 13$ in $\text{PG}(2, 11)$. We have also developed a new classification algorithm for cubic curves in small projective planes. Moreover, a new upper bound is proved for the number of 5-secants of $(45, 5)$ -arc. In addition to proving our new lower bound for the complete $(k, 5)$ -arc in $\text{PG}(2, 11)$. The non existence of $(44, 5)$ -arc and $(45, 5)$ -arc is formulated as a new conjecture for $q = 11$. Using an arc of degree 2 and exploiting the complement relation between arcs and blocking sets we find new 134 isomorphism types of $(77, 8)$ -arcs in $\text{PG}(2, 11)$.

Contents

1	Introduction	10
2	Preliminaries	13
2.1	Finite fields	13
2.2	The projective plane $\text{PG}(2, q)$ over a finite field \mathbf{F}_q	14
2.3	The Principle of Duality	17
2.4	The Fundamental Theorem of Projective Geometry	17
2.5	Plane curves in $\text{PG}(2, q)$	18
2.6	(k, n) –arcs in $\text{PG}(2, q)$	19
2.7	Combinatorics of a (k, n) –arc in $\text{PG}(2, q)$	20
2.8	Links to coding theory	22
2.9	Some definitions and results from group theory	24
3	Classification Results for Arcs of Degree 5 and Length at Most 10	26
3.1	Classification of arcs in projective geometry	27
3.2	The line $\text{PG}(1, 11)$	29
3.3	Arcs of size and degree 5	30
3.4	Arcs of size 6 and degree 5	32
3.5	Arcs of size 7 and degree 5	32
3.6	Arcs of size 8 and degree 5	35
3.7	Arcs of size 9 and degree 5	38
3.8	Arcs of size 10 and degree 5	39
4	Results for arcs of degree 5 and length at most 13	42
4.1	The GAP SCSCP package	42

4.2	The projectively distinct $(11, 5)$ -arcs	43
4.3	The projectively distinct $(12, 5)$ -arcs	49
4.4	The projectively distinct $(13, 5)$ -arcs	53
5	Combinatorial Classification Algorithms for Large Arcs in $\text{PG}(2, q)$	54
5.1	General definitions	54
5.2	Isomorph classification of arcs in $\text{PG}(2, q)$ using canonical forms	57
5.3	Classification of objects in combinatorics	57
5.4	Poset classification	58
5.4.1	Some theory of the Poset classification algorithm	58
6	Application of The Combinatorial Classification Algorithms for Large Arcs in $\text{PG}(2, 11)$	62
6.1	Arcs of degree 3 in $\text{PG}(2, 11)$	62
6.2	Arcs of degree 4 in $\text{PG}(2, 11)$	64
6.3	Arcs of degree 5 in $\text{PG}(2, 11)$	65
6.4	The smallest complete arcs of degree 5 in $\text{PG}(2, 11)$	69
6.5	Large arcs and blocking sets	71
7	Conclusion and Future Work	74
7.1	Conclusions	74
7.2	Recommendation for Future Research	75
	Appendices	77
A	GAP codes and labelling of points in $\text{PG}(2, 11)$	78
A.1	GAP package FinIng labelling [6]	78
A.2	GAP system labelling [35]	79
A.3	Distributed classification of arcs of degree five with GAP and the ScScP package	81
B	Orbiter makefiles and labelling of points	85
B.1	Orbiter labelling of points in $\text{PG}(2, 11)$	85
B.2	Large arcs and blocking sets	86

List of Figures

2.1	The projective plane $\text{PG}(2, 2)$	16
5.1	The adjacency matrix of a Levi graph	56

List of Tables

2.1	$m_n(q)$, $q \leq 13$	22
3.1	Classification methods of arcs in $\text{PG}(2, 11)$	29
3.2	The projectively distinct $(5, 5)$ -arcs in $\text{PG}(2, 11)$	31
3.3	The projectively distinct $(6, 5)$ -arcs in $\text{PG}(2, 11)$	33
3.4	The projectively distinct $(7, 5)$ -arcs in $\text{PG}(2, 11)$	33
3.5	The orbits and points types of $(8, 5)$ -arcs in $\text{PG}(2, 11)$	35
3.6	The projectively distinct $(8, 5)$ -arcs in $\text{PG}(2, 11)$	37
3.7	Orbits of $(8, 5)$ -arcs and their order	38
3.8	The projectively distinct $(9, 5)$ -arcs in $\text{PG}(2, 11)$	38
3.9	The projectively distinct $(10, 5)$ -arcs in $\text{PG}(2, 11)$	39
4.1	The projectively distinct $(11, 5)$ -arcs in $\text{PG}(2, 11)$	43
4.2	Projectively inequivalent $(12, 5)$ -arcs in $\text{PG}(2, 11)$	49
5.1	The orbits $\mathcal{T}_{i,r}$ of $\text{Stab}_G(P_i)$ on $\text{Up}(P_i)$	59
5.2	The orbits $\mathcal{S}_{j,l}$ of $\text{Stab}_G(Q_j)$ on $\text{Down}(Q_j)$	61
6.1	Number of the distinct $(k, 3)$ -arcs in $\text{PG}(2, 11)$	63
6.2	Classification of $(21, 3)$ -arcs in $\text{PG}(2, 11)$	63
6.3	Elliptic curves in $\text{PG}(2, 11)$	64
6.4	Point types of the $(32, 4)$ -arcs	64
6.5	$(32, 4)$ -arcs in $\text{PG}(2, 11)$	64
6.6	Known $(43, 5)$ -arcs in $\text{PG}(2, 11)$	65
6.7	Sharpening of bounds in the proof of Theorem 6.3.1	68
6.8	The column-tactical decomposition scheme in $\text{PG}(2, 11)$	69

6.9	The decomposition of the incidence matrix w.r.t. $(5, 2)$ -arc	72
6.10	The projectively distinct $(77, 8)$ -arcs in $\text{PG}(2, 11)$	72
7.1	The decomposition of the incidence matrix w.r.t. $(9, 2)$ -arcs	76
7.2	The projectively distinct $(9, 2)$ -arcs in $\text{PG}(2, 11)$	76

Chapter 1

Introduction

Finite projective geometries are of modern interest from both pure and applied perspectives. One of the central research directions in finite geometry is concerned with combinatorial structures in finite projective planes: arcs, blocking sets, curves, and many other discrete structures.

In the Desarguesian projective plane $\text{PG}(2, q)$, a set \mathcal{K} of k points is called a (k, n) -arc such that some n , but no $n + 1$, of them are on the same line. Examples of (k, n) -arcs arise from algebraic curves of degree n . The largest value of k for which a (k, n) -arc in $\text{PG}(2, q)$ exists is denoted by $m_n(2, q)$.

Let $\text{PGL}(3, q)$ denote the projective linear group of $\text{PG}(2, q)$, then two arcs \mathcal{K}_1 and \mathcal{K}_2 in $\text{PG}(2, q)$ are projectively equivalent if there exists an element $\alpha \in \text{PGL}(3, q)$ such that $\mathcal{K}_1^\alpha = \mathcal{K}_2$. The classification problem of (k, n) -arcs is to determine the distinct (k, n) -arcs up to projective equivalence.

For $n = 2$, a considerable deal of research has been done in classifying arcs for $q = 2, 3, 5, 7, 9, 11, 13$ - for details of the related results see [33]. The result of Segre [33] shows that every $(q+1)$ -arc in $\text{PG}(2, q)$ is a conic, for q odd. When q is even, the situation is more complicated. In this case, the largest arcs are hyperovals, which consist of $q+2$ points. For $q = 2, 4, 8$, all hyperovals have the form conic plus nucleus and are unique. For $q \geq 16$, the situation becomes very complicated - for further information see [12] and [18]. Coolsaet and Sticker [14] classifies degree 2 arcs - for $q = 23, 25$.

For $n = 3$ with $q = 5$, Yazdi [37] study the classification of (k, n) -arcs. For $q = 7, 8, 9$ the

classification was done by Marcugini [27]. Marcugini [28] also classifies degree 3 arcs with $q = 13$. Cook [13] studies $m_n(2, 11)$ for $n \leq 4$, and finds four isomorphism types of $(32, 4)$ -arcs in $\text{PG}(2, 11)$. Cook also classifies the $(21, 3)$ -arcs in $\text{PG}(2, 11)$ - up to isomorphism there are exactly two such arcs. In 2003, Hill and Love [21] classified $(22, 4)$ -arcs for $q = 7$.

Regarding the problem of classification of arcs of degree 5 much less is known. Ball [3] shows that $43 \leq m_5(2, 11) \leq 45$ and gives one example of a $(43, 5)$ -arc. This motivates us to work on the classification of $(k, 5)$ -arcs in $\text{PG}(2, 11)$ and then to investigate combinatorial and algebraic approaches to construct (k, n) -arcs of degree $n \geq 5$.

In Chapter 2, we introduce some preliminary definitions, lemmas and theorems related to projective planes over finite fields, plane curves and (k, n) -arcs in $\text{PG}(2, q)$, group theory, in addition, to presenting the main application of studying (k, n) -arcs in coding theory. These preliminaries are needed to understand the research done in later chapters.

In Chapter 3, we classified $(k, 5)$ -arcs where $k = 6, 7, \dots, 10$ in $\text{PG}(2, 11)$ using the open-source software package GAP [35].

In Chapter 4, the classification of $(k, 5)$ -arcs is continued for $k = 11, 12, 13$. A similar program as in the classification of $(k, 5)$ -arcs in Chapter 3 is used but with parallel processing using the GAP ScScp package [26]. The program is included in Appendix A.3. As the complexity of the calculations grew exponentially the list of arcs was no longer fitting into the main memory. So we decided we could not use GAP after $k = 13$. The next stage where $k = 14$ would be beyond practical reachability.

In Chapter 5, we continued investigating with the software package Orbiter [10] developed by *Anton Betten* from Colorado State University. Cook's classification of degree 3 arcs [13] was important to our work as we are interested in (k, n) -arcs where $n > 3$ and $q = 11$. Therefore we started verifying Cook's results using a different technique in Orbiter. This technique is called Poset classification explained in Section 5.4. This algorithm creates and classifies combinatorial objects at the same time. It operates to work particularly well on problems in finite geometry. We used Orbiter in parallel on the Sussex cluster to classify the arcs of degree 4. This classification was based on extending all isomorphism types of $(k, 3)$ -arcs, both complete and incomplete. These results are presented in Section 6.1.

So far, no $(44, 5)$ -arc nor $(45, 4)$ -arc are known, but they have not been ruled out either. We formulate a new conjecture that may be none of them exists. We have been able to get

a new example of a $(43, 5)$ -arc by extending the first complete $(32, 4)$ -arc from Cook's list. However the other Cook's arcs did not extend.

No $(32, 4)$ -arcs in $\text{PG}(2, 11)$ extend to a $(45, 5)$ -arc, but this does not mean that there are none. However, using systems of Diophantine equations, we give a new lower bound for the number of 5-secants in a putative $(45, 5)$ -arc. This is a small contribution to the problem of deciding the existence of a $(45, 5)$ -arc.

Section 6.5 describes a technique due to Hill and Ball [3] to construct large arcs and multiple blocking sets. This technique gives multiple isomorphism types of new arcs. We now include this algorithm in the Orbiter library as a new tool to find large arcs and blocking sets. A list of the classification and the construction program code in a makefile are presented in Appendix B.2.

Chapter 2

Preliminaries

2.1 Finite fields

Definition 2.1.1. (Finite field)

A field \mathbf{F} is a set on which two binary operations are defined $(+, \cdot)$ such that

- (a) $(\mathbf{F}, +)$ is a commutative group where the additive identity of \mathbf{F} is 0;
- (b) $(\mathbf{F} \setminus \{0\}, \cdot)$ is a commutative group where the multiplicative identity of \mathbf{F} is 1;
- (c) multiplication is distributive over addition.

Definition 2.1.2. The *order* of a field is the number of elements in that field. A *finite field* is a field which has a finite number of elements.

Definition 2.1.3. Let \mathbf{F} be a finite field; then the characteristic of \mathbf{F} is the smallest positive integer n such that

$$\underbrace{1 + 1 + \cdots + 1}_{n\text{-times}} = n = 0.$$

Proposition 2.1.4. For a prime number p , a field \mathbf{F} of characteristic p the elements $0, 1, \dots, p-1$ form a subfield isomorphic to $\mathbf{F}_p = \mathbb{Z}/(p)$; the Galois field of order p .

Theorem 2.1.5. A field \mathbf{F} with q elements has characteristic p where p is prime number and $q = p^h$.

Proof See [4].

□

Definition 2.1.6. A field automorphism is an isomorphism from the field to itself. The set of all automorphisms form a group under the composition as a binary operation.

The group $Aut(\mathbf{F}_q)$ of automorphisms of \mathbf{F}_q is generated by $\sigma(x) = x^p$:

$$Aut(\mathbf{F}_q) = \{I, \sigma, \sigma^2, \dots, \sigma^{h-1}\}$$

2.2 The projective plane $PG(2, q)$ over a finite field \mathbf{F}_q

Let \mathbf{F}_q be the finite field of q elements and let \mathbf{F}_q^n be the set of all n -tuples over \mathbf{F}_q . The elements of \mathbf{F}_q are called scalars and the elements of \mathbf{F}_q^n are called vectors.

Definition 2.2.1. (Vector space)

A vector space or a linear space $V(n, q)$, $q = p^h$, is the set of all vectors in V over a finite field \mathbf{F}_q that satisfy the following axioms:

1. $V(n, q)$ is an abelian group additively; that is, for all $u, v, w \in V(n, q)$ and for all $a, b \in \mathbf{F}_q$;
 - (a) closure property under addition: if $u, v \in V$ then $u + v \in V$;
 - (b) associative property under addition: $u + (v + w) = (u + v) + w$;
 - (c) additive identity: for all $u \in V(n, q)$, $u + 0 = 0 + u$;
 - (d) additive inverse: for all $u \in V(n, q)$, there exists $-u \in V(n, q)$ such that $u + (-u) = 0$;
 - (e) commutativity under addition: $u + v = v + u$, for all $u, v \in V$;
2. scalar multiplication:
 - (a) closure property under scalar multiplication: $au \in V(n, q)$, for all $a \in \mathbf{F}_q$ and $u \in V$;
 - (b) $a(bu) = (ab)u$;
 - (c) identity under scalar multiplication: $1u = u$, for all $u \in V$ and 1 is the multiplicative identity of \mathbf{F}_q ;

3. distributive property:

(a) distribution of scalar multiplication over addition: $a(u + v) = (au) + (av)$ for all $a \in \mathbf{F}_q$ and $u, v \in V(n, q)$;

(b) distribution of scalar addition over vector multiplication: $(a + b)u = (au) + (bu)$ for all $a, b \in \mathbf{F}_q$ and $u \in V(n, q)$;

Definition 2.2.2. The vectors $v_1, v_2, \dots, v_k \in V$ are *linearly dependent* if there exists $\lambda_1, \lambda_2, \dots, \lambda_k \in \mathbf{F}_q$ not all zero such that

$$\lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_k v_k = 0.$$

Definition 2.2.3. A subset $S = \{v_1, v_2, \dots, v_k\}$ of V , is called a *spanning set* of V if every vector in V can be written as a linear combination of the vectors in S .

Definition 2.2.4. 1. The subset $S = \{v_1, v_2, \dots, v_k\}$ of V , is called a *basis* of V if the vectors of S form a spanning set of V and they are linearly independent.

2. The vector space V over a field F is called finite dimensional if its spanning set has a finite number of vectors.

Definition 2.2.5. The dimension of a finite dimensional vector space V is the number of elements in its basis.

Definition 2.2.6. (subspace)

A subset of $V(n, q)$ is a *subspace* if it is a vector space itself under the same operations; that is, the addition and scalar multiplication.

Lemma 2.2.7. Let \mathbf{F} be a finite field of characteristic p ; then \mathbf{F} is a vector space over \mathbf{F}_p .

Definition 2.2.8. Let $V = V(3, q) = \{(x_0, x_1, x_2), x_i \in \mathbf{F}_q\}$ be a 3-dimensional vector space over the finite field \mathbf{F}_q of order q , where $q = p^h$, p is prime and h is a positive integer. So points in $\text{PG}(2, q)$ correspond to the one-dimensional subspaces of V . Also, lines in $\text{PG}(2, q)$ correspond to the two-dimensional subspaces of V . The point P is said to be incident with the line L if and only if P is a subspace of L .

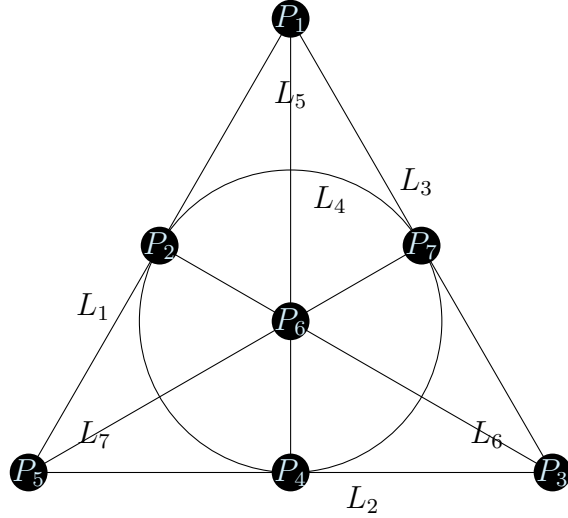


Figure 2.1: The projective plane $\text{PG}(2, 2)$

The algebraic representations of points and lines in $\text{PG}(2, q)$ is shown in the following definition.

Definition 2.2.9. (a) a point of $\text{PG}(2, q)$ is $\mathbf{P}(x, y, z) \neq (0, 0, 0)$ where $\mathbf{P}(\lambda x, \lambda y, \lambda z) = \mathbf{P}(x, y, z)$ and $\lambda \in \mathbf{F}_q \setminus \{0\}$.

(b) The lines are $uX + vY + wZ = \{\mathbf{P}(x, y, z) \mid ux + vy + wz = 0\}$.

Lemma 2.2.10. *The following are basic properties of $\text{PG}(2, q)$.*

(a) *The number of points in $\text{PG}(2, q)$ is $q^2 + q + 1$.*

(b) *The number of lines in $\text{PG}(2, q)$ is $q^2 + q + 1$.*

(c) *There are $q + 1$ points on a line in $\text{PG}(2, q)$.*

(d) *There are $q + 1$ lines through a point in $\text{PG}(2, q)$.*

Example 2.2.11. The set $\text{PG}(2, 2)$ consists of seven points $P_1, P_2, P_3, P_4, P_5, P_6, P_7$. A visual representation is given by Figure 2.1. In this figure, the L_i where $i = \{1, \dots, 7\}$ represent the lines of the plane.

Definition 2.2.12. (Incidence matrix)

For a projective plane $\text{PG}(2, q)$ with the set $\{P_1, P_2, \dots, P_{q^2+q+1}\}$ of points and the set $\{L_1, L_2, \dots, L_{q^2+q+1}\}$, of lines then $A = (a_{ij})$ is the $(q^2 + q + 1) \times (q^2 + q + 1)$ incidence matrix. Its entries, a_{ij} , are defined as follows:

$$a_{ij} = \begin{cases} 1 & \text{if } P_i \text{ and } L_j \text{ are incident} \\ 0 & \text{otherwise.} \end{cases}$$

Example 2.2.13. For $\text{PG}(2, 2)$ in Example 2.2.11, the 7×7 incidence matrix is as follows:

$$A_7 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

2.3 The Principle of Duality

For any projective plane $\Pi = \text{PG}(2, q)$, there is a dual plane Π^* . Let S be any statement that is valid in Π and let S^* be its dual statement defined by replacing each occurrence, in S , of the word ‘line’ by the word ‘point’ and each ‘point’ by ‘line’. Then S^* also holds in Π .

2.4 The Fundamental Theorem of Projective Geometry

Definition 2.4.1. Let M be a non-singular 3×3 matrix over \mathbf{F}_q , $q = p^h$ then the one-to-one map from $\text{PG}(2, q)$ onto itself defined by

$$\alpha \mathbf{P}(X) = M \mathbf{P}(X') \quad \text{where } \mathbf{P}(X) = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \quad \mathbf{P}(X') = \begin{bmatrix} x' \\ y' \\ z' \end{bmatrix}$$

is called a *projectivity* of $\text{PG}(2, q)$. The group of all projectivities of $\text{PG}(2, q)$ is denoted by $\text{PGL}(3, q)$ and called the *projective linear group*.

Definition 2.4.2. A *collineation* of a projective plane Π onto itself is a bijective mapping such that the images of collinear points are collinear.

Definition 2.4.3. (Collineation group)

The group of collineations of $\Pi = \text{PG}(2, q)$ is denoted by $\text{PGGL}(3, q)$.

Theorem 2.4.4. (*The Fundamental Theorem of Projective Geometry*)

1. If $\{\mathbf{P}_0, \mathbf{P}_1, \dots, \mathbf{P}_{n+1}\}$ and $\{\mathbf{P}'_0, \mathbf{P}'_1, \dots, \mathbf{P}'_{n+1}\}$ are both subsets of $\text{PG}(n, q)$ of size $n+2$ such that no $n+1$ of which are in the same hyperplane, then there is a unique projectivity \mathfrak{T} such that $\mathbf{P}'_i = \mathbf{P}_i \mathfrak{T}$.
2. For $n = 1$, (1.) implies that: there is a unique projectivity that transforms any three distinct points on a line to any other 3 points.
3. For $n = 2$, (1.) implies that: there is a unique projectivity that transforms any four distinct points no three of which are collinear to any other 4 points no three of them are collinear.

Definition 2.4.5. A projective frame or what we call the *standard frame* of a projective plane $\text{PG}(2, q)$ is an ordered set of 4 points of which no 3 of them are on the same line.

2.5 Plane curves in $\text{PG}(2, q)$

Definition 2.5.1. A homogeneous polynomial or a form in $\text{PG}(2, q)$ is a polynomial with a number of variables and coefficients in \mathbf{F}_q where every term has the same degree.

Definition 2.5.2. Let n be a positive integer, a projective plane curve in $\text{PG}(2, q)$ is the zero set of a homogeneous polynomial ϕ of degree n in the 3 variables X_0, X_1, X_2 over a finite field \mathbf{F}_q . So

$$\phi(X) = \sum a_{i_0, i_1, i_2} X_0^{i_0} X_1^{i_1} X_2^{i_2}$$

where $a_{i_0, i_1, i_2} \in \mathbf{F}_q$, $n = i_0 + i_1 + i_2$. Also, ϕ has $\binom{2+n}{n}$ terms if all coefficients are non-zero.

Example 2.5.3. A curve C of degree 2 in $\text{PG}(2, \mathbf{F}_q)$ is the set of points satisfying $\phi(X_0, X_1, X_2) = 0$, where ϕ is a non-zero homogeneous polynomial of degree 2.

Definition 2.5.4. If the non-zero homogeneous polynomial equation of the plane curve C is of degree 2 then the equation of the conic C is of the form:

$$\phi = a_{00}X_0^2 + a_{11}X_1^2 + a_{22}X_2^2 + a_{01}X_0X_1 + a_{02}X_0X_2 + a_{12}X_1X_2$$

or equivalently when the field characteristic $p \neq 2$,

$$\phi = X^t A X, \quad \text{where } A = \begin{pmatrix} a_{00} & a_{01}/2 & a_{02}/2 \\ a_{01}/2 & a_{11} & a_{12}/2 \\ a_{02}/2 & a_{12}/2 & a_{22} \end{pmatrix} \text{ is a symmetric matrix and}$$

$$X = \begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix} \text{ is the point } \mathbf{P}(X_0, X_1, X_2) \text{ in a column form.}$$

Definition 2.5.5. (conics in $\text{PG}(2, q)$)

Let $\text{PG}(2, q)$ be the projective plane over finite field of odd characteristic then a conic is the zero set of a non-degenerate quadratic form over \mathbf{F}_q ; that is, the matrix A is non-singular.

Example 2.5.6. In a projective plane $\text{PG}(2, q)$, a conic has 6 terms and a quintic has 21 terms.

Theorem 2.5.7. (*Bézout's theorem*)

In $\text{PG}(2, \mathbf{F})$, let C^n, C^m be curves of degrees n and m . Suppose they have no common component. Then, they intersect in mn points, some possibly belonging to $\text{PG}(2, E) \setminus \text{PG}(2, \mathbf{F})$, where E is an extension of \mathbf{F} .

Proof See [16]. □

2.6 (k, n) -arcs in $\text{PG}(2, q)$

Definition 2.6.1. A (k, n) -arc \mathcal{K} in $\text{PG}(2, q)$, the projective plane of order q , is a set of k points no $(n+1)$ of which are collinear but some n of which are collinear.

Example 2.6.2. For $n = 2$, a $(k, 2)$ -arc is a set of k points in $\text{PG}(2, q)$, no three of which are collinear but there is at least 2 points on the same line. It is simply called a k -arc.

Definition 2.6.3. (Ovals in $\text{PG}(2, q)$)

A $(q + 1, 2)$ –arc in $\text{PG}(2, q)$ is called an oval.

Definition 2.6.4. An (n, k) –arc is *complete* if it is maximal with respect to inclusion, that is, there is no $(n + 1, k)$ –arc containing it.

Definition 2.6.5. In $\text{PG}(2, q)$, the size of the largest complete arc of degree r is denoted by $m_r(2, q)$.

Theorem 2.6.6. (Bose [11]).

In $\text{PG}(2, q)$, the largest arc of degree 2 has $q + 1$ points for q odd. The largest arc of degree 2 has $q + 2$ points for q even.

$$m_2(2, q) = \begin{cases} q + 1 & \text{if } q \text{ is odd} \\ q + 2 & \text{if } q \text{ is even} \end{cases}$$

Theorem 2.6.7. (Segre [33]). For q odd, every $(q + 1)$ –arc is a conic.

Definition 2.6.8. (t -fold blocking set)

A set B in a finite projective plane $\text{PG}(2, q)$ is called a t -fold blocking set if the following two properties hold:

- i. each line in $\text{PG}(2, q)$ has at least t points of B that is, $|l \cap B| \geq t$;
- ii. there exists a line that intersects B in exactly t points.

Note 2.6.9. In $\text{PG}(2, q)$, the following hold:

- 1. the complement of a t -fold blocking set B is a $(q^2 + q + 1 - |B|, q + 1 - t)$ –arc;
- 2. the complement of a (k, n) –arc is a t -fold blocking set with $t + n = q + 1$ and $|B| = q^2 + q + 1 - k$.

2.7 Combinatorics of a (k, n) –arc in $\text{PG}(2, q)$

Let l be a line in $\text{PG}(2, q)$ with $|l \cap \mathcal{K}| = i$; then l is called an i -secant of \mathcal{K} . Let \mathcal{K} be a (k, n) –arc in $\text{PG}(2, q)$

Definition 2.7.1. 1. Let τ_i denote the number of i -secants of \mathcal{K} . Then the *secant distribution* of \mathcal{K} is $[\tau_0, \tau_1, \dots, \tau_{n-1}, \tau_n]$ or $[n^{\tau_n}, (n - 1)^{\tau_{n-1}}, \dots, 2^{\tau_2}, 1^{\tau_1}, 0^{\tau_0}]$.

2. Let ρ_i denote the number of i -secants of \mathcal{K} through a point p in \mathcal{K} ; then the *arc points type* is $[\rho_0, \rho_1, \dots, \rho_{n-1}, \rho_n]$ or $[n^{\rho_n}, (n-1)^{\rho_{n-1}}, \dots, 2^{\rho_2}, 1^{\rho_1}]$.
3. Let $\sigma_i = \sigma_i(x)$ denote the number of i -secants through the point $x \in \text{PG}(2, q) \setminus \mathcal{K}$; then the number of n -secants through x is called the index of x for \mathcal{K} .

Lemma 2.7.2. (*Hirschfeld [22]*). *For a (k, n) -arc \mathcal{K} in $\Pi = \text{PG}(2, q)$ the following equations hold.*

$$\sum_{i=0}^n \tau_i = q^2 + q + 1; \quad (2.1)$$

$$\sum_{i=1}^n i\tau_i = k(q+1); \quad (2.2)$$

$$\sum_{i=0}^n (q+1-i)\tau_i = (q^2 + q + 1 - k)(q+1); \quad (2.3)$$

$$\sum_{i=2}^n \binom{i}{2} \tau_i = \binom{k}{2}; \quad (2.4)$$

$$\sum_{i=0}^n \binom{q+1-i}{2} \tau_i = \binom{q^2 + q + 1 - k}{2}; \quad (2.5)$$

$$\sum_{i=0}^n i(q+1-i)\tau_i = k(q^2 + q + 1 - k). \quad (2.6)$$

Proof The six equations give the cardinality of the following sets:

1. $\{x \mid x \in \Pi\}$;
2. $\{(p, l) \mid p \in l \cup \mathcal{K}, l \text{ is an } i\text{-secant of } \mathcal{K}\}$;
3. $\{(x, l) \mid x \in (l \cup \Pi \setminus \mathcal{K}), l \text{ is an } i\text{-secant of } \mathcal{K}\}$;
4. $\{(p, p', l) \mid p \neq p', p, p' \in \mathcal{K} \text{ and } p, p' \in l\}$;
5. $\{(x, x', l) \mid x \neq x', x, x' \in \Pi \setminus \mathcal{K} \text{ and } x, x' \in l\}$;
6. $\{(p, x, l) \mid p \in (l \cup \mathcal{K}) \text{ and } x \in l\}$;

□

Table 2.1 shows the values of $m_n(2, q)$ for $q \leq 13$, or upper and lower bound if the exact value is unknown.

Table 2.1: $m_n(q)$, $q \leq 13$

q	2	3	4	5	7	8	9	11	13
n									
2	4	4	6	6	8	10	10	12	14
3	7	9	9	11	15	15	17	21	23
4		13	16	16	22	28	28	32	38 – 40
5			21	25	29	33	37	43 – 45	49 – 53
6				31	36	42	48	56	64 – 66
7					49	49	55	67	79
8					57	64	65	78	92
9						73	81	89 – 90	105
10							91	100 – 102	118 – 119
11								121	132 – 133
12								133	145 – 147

2.8 Links to coding theory

Nowadays, the problem of coding and decoding of transmitted data over a noisy communication channel is very difficult. The communication needs to be done as quickly and as reliably as possible. Due to the fact that there is no ideal channel this data is exposed to distortion. Therefore the recipient may make errors in decoding the original transmitted message. One of the central problems in coding theory is to reduce these errors. Namely, sending messages that arrive with the same content as when they were sent.

Linear codes

Let $V(n, q) = \mathbf{F}_q^n$ with $q = p^h$. A linear $[n, k]$ code \mathcal{C} of length n and dimension k is a k -dimensional subspace of the n -dimensional vector space $V = V(n, q)$. The elements of \mathcal{C} are called code-words. The Hamming distance $d(c_1, c_2)$ between any two elements $c_1, c_2 \in \mathcal{C}$ is the number of coordinates in which they differ. The minimum distance d of the code \mathcal{C} is the minimum Hamming distance between any two code-words of \mathcal{C} . Equivalently, d is the smallest number of non-zero symbols in any non-zero element of \mathcal{C} . The *Singleton bound* is that $d \leq n - k + 1$. Furthermore, two linear codes in $V = V(n, q)$ are called equivalent if one can be obtained from the other by the following:

- a permutation of the coordinates;

- multiplying a coordinate by a non-zero element in \mathbf{F}_q .

Lemma 2.8.1. *If a code \mathcal{C} has minimum distance d , then it can correct $e = \lfloor \frac{(d-1)}{2} \rfloor$ errors, where $\lfloor x \rfloor$ denotes the integer part of x .*

m -arcs and linear MDS codes

An $(m, 2)$ -arc in $\text{PG}(2, q)$ is a set of m points in which at most 2 points on the same line but there exists two points on the same line. For simplicity, we refer to an $(m, 2)$ -arc as an m -arc. A $[n, 3, d]$ code \mathcal{C} in $\text{PG}(2, q)$ is called a *maximum distance separable* code (MDS) if it meets the Singleton bound. That is, the minimum distance $d(\mathcal{C}) = n - 2$. A generator matrix G of the code \mathcal{C} is a $3 \times n$ matrix whose rows form a basis for \mathcal{C} . Then \mathcal{C} is an MDS code if and only if any 3 columns of G are linearly independent; this property is preserved under multiplication of the columns by non-scalars. So consider the columns of G as points P_1, P_2, \dots, P_m of $\text{PG}(2, q)$. It follows that \mathcal{C} is an MDS if and only if $\{P_1, \dots, P_m\}$ is an m -arc of $\text{PG}(2, q)$. Namely, an m -arc corresponds to a $[m, 3, m - 2]$ MDS code. This gives the relation between linear MDS codes and arcs of degree 2 in $\text{PG}(2, q)$ which are equivalent objects.

Example 2.8.2. Let $\text{PG}(2, 3)$ be the projective plane over finite field of 3 elements then an $(4, 2)$ -arc = $\{\mathbf{P}(1, 0, 0), \mathbf{P}(0, 1, 0), \mathbf{P}(1, 1, 0), \mathbf{P}(0, 0, 1), \mathbf{P}(1, 1, 1)\}$; corresponds to an $[4, 3, 2]$ MDS code \mathcal{C} with a generator matrix G as follows:

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Where each point of the arc represent a column in G . The minimum distance $d(\mathcal{C}) = 2$ since any two columns of G differs in two coordinates. The linear code \mathcal{C} is an MDS code as its minimum distance d attain the singleton bound.

An $(n, n - d)$ -arc in $\text{PG}(2, q)$ is equivalent to a linear $[n, 3, d]$ code. For detailed information about the link between a linear $[n, 3, d]$ -code and $(n, n - d)$ -arc see [5].

Finding the maximal arcs with respect to inclusion corresponds to finding the largest linear codes that cannot be extended to a larger one with the same minimum distance.

For instance, our new example of the complete $(43, 5)$ -arc in $\text{PG}(2, 11)$ listed in Table 6.6 corresponds to the linear $[43, 3, 38]$ -code which can not be extended to a larger code with minimum distance equal to 38 and according to Corollary 2.8.1 it can correct 18 errors. Moreover, the four isomorphism types of $(32, 4)$ -arcs in $\text{PG}(2, 11)$ that we classified in Section 6.2 can be viewed as the linear $[32, 3, 28]$ -codes with minimum distance of 28 and can correct 13 errors.

2.9 Some definitions and results from group theory

Definition 2.9.1. Let G be a group, X be non-empty set. We say that G acts on X (or G permutes X) if for all $g \in G$ and $x \in X$ there exists a unique $xg \in X$ such that for all $x \in X$ and $g_1, g_2 \in G$

1. $(xg_1)g_2 = x(g_1g_2)$.

2. $x1 = x$.

Lemma 2.9.2 ([31]). *Let G acts on X . We define a relation \sim on X by setting $x_1 \sim x_2 \iff x_1, x_2 \in X$ and there exists an element $g \in G$ such that $x_1g = x_2$. Then \sim is an equivalence relation on X .*

Definition 2.9.3. Let G act on the set X . Then X is partitioned into disjoint equivalence classes with respect to the equivalence relation \sim of Lemma 2.9.2. These equivalence classes are called orbits or transitivity classes of the action.

The *orbit* of x is $\text{Orb}_G(x) = \{xg : g \in G\}$. The set $\text{Stab}_G(x) = \{g \in G : xg = x\}$. Then $\text{Stab}_G(x)$ is a subgroup of G , called the stabilizer of x in G .

Theorem 2.9.4 ([31]). *Let G act on the set X , and let $x \in X$. Then*

$$|G| = |\text{Stab}_G(x)| \cdot |\text{Orb}_G(x)|.$$

Theorem 2.9.5 ([31]). *(Conjugate-Stabilizer Theorem)*

Consider the finite group G acting on the finite set X and let $x \in X$ and let $g \in G$. Then,

$$\text{Stab}_G(xg) = g^{-1}\text{Stab}_G(x)g.$$

Groups of small orders appear periodically in later chapters and here is a list of those groups that show up:

$$C_n = \text{cyclic group of order } n;$$

$$\begin{aligned} D_{2n} &= \text{dihedral group of order } 2n \\ &= \langle a, b \mid a^n = b^2 = 1, bab^{-1} = 1 \rangle; \end{aligned}$$

$$A \times B = \text{direct product of } A \text{ and } B;$$

$$A \rtimes B = \text{semi-direct product of } A \text{ and } B.$$

Chapter 3

Classification Results for Arcs of Degree 5 and Length at Most 10

In this chapter, we will describe our procedures to find and classify arcs of degree 5 and length at most 10 in $\text{PG}(2, 11)$. To program these procedures, we use the open-source software package GAP [35].

Let \mathcal{K} be a $(k, 5)$ -arc together with the set S_k of the 5-secants of \mathcal{K} . The new $(k+1, 5)$ -arcs are generated by the action of $G(\mathcal{K})$, the projective subgroup fixing \mathcal{K} , on the set of points in $\text{PG}(2, 11) \setminus \{\mathcal{K} \cup S_k\}$. By excluding the set $\{\mathcal{K} \cup S_k\}$, we make sure that the new $(k+1, 5)$ -arcs do not have 6 points on the same line.

The set $\text{PG}(2, 11) \setminus \{\mathcal{K} \cup S_k\}$ is partitioned into the group orbits $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_r$. Next, a point x would be chosen from each orbit \mathcal{O}_i for $i = 1, \dots, r$ and added to \mathcal{K} to get the extended $(m, 5)$ -arcs in the list $R = \{\mathcal{K} \cup \{x_1\}, \mathcal{K} \cup \{x_2\}, \dots, \mathcal{K} \cup \{x_r\}\}$ where $m = 6, 7, \dots, 10$. This procedure is described briefly in Algorithm 1.

Then, we classify the new $(m, 5)$ -arcs in R by determining the projectively inequivalent ones as it is shown in Algorithm 2 using the GAP function `CanonicalImage` explained in Section 3.1

Algorithm 1: Extending $(k, 5)$ -arcs in $\text{PG}(2, 11)$

Data: A list of $(k, 5)$ -arcs and a set S_k of the 5-secants in $\text{PG}(2, 11)$

Result: A list R of all the $(k + 1, 5)$ -arcs

$R := \emptyset;$

for each $(k, 5)$ -arc **do**

while $\text{PG}(2, 11) \setminus \{(k, 5)\text{-arc} \cup S_k\} \neq \emptyset$ **do**

 Compute orbits of $\text{Stab}_G((k, 5)\text{-arc})$ on $\text{PG}(2, 11) \setminus \{(k, 5)\text{-arc} \cup S_k\}$

Add a point from each orbit to the $(k, 5)$ -arc to obtain a $(k + 1, 5)$ -arc.

Add($R, (k + 1, 5)\text{-arc}$)

end

end

Algorithm 2: Classify the list of arcs in R up to projective equivalence.

Data: A list R of all the new $(k + 1, 5)$ -arcs

Result: A list M of all the projectively distinct $(k + 1, 5)$ -arc in $\text{PG}(2, 11)$

$M := \emptyset;$

for each $(k + 1, 5)$ -arc in R **do**

 Compute $\mathcal{C}((k + 1, 5)\text{-arc})$

 Where $\mathcal{C}((k + 1, 5)\text{-arc})$ is the canonicalImage of $(k + 1, 5)$ -arc.

AddSet($M, (k + 1, 5)\text{-arc}$)

end

3.1 Classification of arcs in projective geometry

In projective geometry, two sets of points are called projectively equivalent if there exists a projectivity which maps one to the other. This relation is an equivalence relation on sets; so it is reflexive, symmetric, and transitive.

In projective planes, testing if two sets are projectively equivalent can be done by considering quadrangles. If Q_1 and Q_2 are two quadrangles in $\text{PG}(2, q)$ then a projectivity T can be found which maps Q_1 to Q_2 . For this reason, it suffices to consider one quadrangle Q_1 in A and test all quadrangles Q_2 in B to check whether the projectivity T maps Q_1 to Q_2 . So the number of quadrangles to consider is $\binom{|B|}{4}$. Note that the labelling of the points of $\text{PG}(2, 11)$ in GAP is different from the FinInG package [6] as it is shown in Appendix A.2.

Algorithm 3: Check the projectively equivalence relation

Input: Two sets A and B

Output: Whether they are projectively equivalent or not

Find a quadrangle $Q_1 \in A$

and all quadrangles $Q_2 \in B$

for all $Q_2 \in B$ **do**

 Compute a 3×3 matrix T

if $T(Q_1) \neq T(Q_2)$ **then**

 {to skip the rest of the loop}

else if $T(Q_1) = T(Q_2)$ **and** $T(A \setminus Q_1) = T(B \setminus Q_2)$ **then**

return A and B are projectively equivalent.

end if

end for

return A and B are projectively distinct.

Algorithm 3 has been implemented in GAP to check the projective equivalence relation among arcs in the list R . In addition, there are two other built-in functions in GAP: `RepresentativeAction` and `CanonicalImage`.

`RepresentativeAction` checks whether a group element maps one set to the other exists or not.

`CanonicalImage` is part of the GAP package Images [25]. The way that this function works is by computing a canonical image for each arc in R under the group action of $G(\mathcal{K})$: if two arcs have the same canonical image then they are isomorphic, otherwise they are not. For more details see [24].

Example 3.1.1. Let A and B be the following two $(8, 5)$ -arcs in $\text{PG}(2, 11)$:

$$A = \{\mathbf{P}(1, 0, 0), \mathbf{P}(0, 1, 0), \mathbf{P}(0, 0, 1), \mathbf{P}(1, 1, 1), \mathbf{P}(1, 7, 0), \mathbf{P}(1, 2, 0), \mathbf{P}(1, 3, 0), \mathbf{P}(0, 1, 6)\},$$

$$B = \{\mathbf{P}(1, 0, 0), \mathbf{P}(0, 1, 0), \mathbf{P}(0, 0, 1), \mathbf{P}(1, 1, 1), \mathbf{P}(1, 7, 0), \mathbf{P}(1, 9, 0), \mathbf{P}(1, 6, 9), \mathbf{P}(1, 1, 0)\}$$

Using the quadrangles test, the `RepresentativeAction` and `CanonicalImage` functions, we find that A and B are projectively equivalent. Table 3.1 presents an interesting comparison among the runtimes, the time spent by GAP in doing these tests in milliseconds.

Evidently, the `CanonicalImage` is much faster than the other two options as shown in

Table 3.1: Classification methods of arcs in $\text{PG}(2, 11)$

Method	Runtime
Quadrangle test	39
<code>RepresentativeAction</code>	26
<code>CanonicalImage</code>	12

Table 3.1 so that we used it to classify all arcs of degree 5 we get in Chapter 3 and 4 using the points labelling in Appendix B.1.

Let C_0^{k-1} be the subset of $\text{PG}(2, 11) \setminus \{\mathcal{K} \cup S_k\}$ consisting of points in $\text{PG}(2, 11)$ that are off the arc \mathcal{K} and lie on no 5-secants of \mathcal{K} . Write $c_0 = |C_0^{k-1}|$.

3.2 The line $\text{PG}(1, 11)$

On $\text{PG}(1, 11)$, the projective line L_0 over the field of order 11, there are 12 points, namely, $\mathbf{P}(X_0, X_1)$ where $X_i \in \mathbf{F}_{11}$. The non-homogeneous coordinate X_0/X_1 , $X_1 \neq 0$ identifies each point on L_0 with elements of $F_{11} \cup \{\infty\}$. When $X_1 = 0$, the point $\mathbf{P}(\infty, 1) = \{\mathbf{U}_0 = \mathbf{P}(1, 0)\}$. The points $\mathbf{U}_0 = \mathbf{P}(1, 0)$, $U_1 = \mathbf{P}(0, 1)$, and $U = \mathbf{P}(1, 1)$ are called the reference points with respect to the line $\text{PG}(1, 11)$. Let $X = X_0/X_1$, then

$$\text{PG}(1, 11) = \{\mathbf{U}_0 = \mathbf{P}(1, 0)\} \cup \{(X, 1) \mid X \in \mathbf{F}_{11}\}$$

Alternatively, the points on the line L_0 can be identified with elements of F_{11} and the element ∞ as follows:

$$\mathbf{F}_{11} \cup \{\infty\} = \{\infty, 0, \pm 1, \pm 2, \pm 3, \dots, \pm 5\}.$$

A k -set which is an unordered set of k points of $\text{PG}(1, 11)$ can be constructed by adding to any $(k - 1)$ -set one point from the remaining $12 - (k - 1)$ points in $\text{PG}(1, 11)$. A pentad is an unordered set of 5 points of a projective line. On the line $\text{PG}(1, 11)$, there are two projectively distinct pentads, due to [22], of the canonical forms:

$$\mathcal{P}_1 = \{\mathbf{P}(1, 0), \mathbf{P}(0, 1), \mathbf{P}(1, 1), \mathbf{P}(-1, 1), \mathbf{P}(2, 1)\},$$

$$\mathcal{P}_2 = \{\mathbf{P}(1, 0), \mathbf{P}(0, 1), \mathbf{P}(1, 1), \mathbf{P}(-2, 1), \mathbf{P}(3, 1)\}$$

The pentad \mathcal{P}_1 has a projective group $G(\mathcal{P}_1)$ isomorphic to $Z_2 = \langle x \mapsto 1 - x \rangle$ and 660 is the number of elements in the orbit on L_0 , that is $|\text{PGL}(2, 11)| \div |Z_2|$. The group of \mathcal{P}_2 is $G(\mathcal{P}_2) = \langle x \mapsto -2/x, x \mapsto (x+2)/x \rangle \cong D_{10}$ and $|\text{PG}(2, 11)| \div |D_{10}| = 132$ is the cardinality of the orbit on $\nu(Z)$. Here $G(\mathcal{P}_1)$ and $G(\mathcal{P}_2)$ are subgroups of the projective general linear group $\text{PGL}(2, 11)$.

Let G_{L_i} be the stabiliser in $\text{PGL}(3, 11)$ of a line $L_i \in \text{PG}(2, 11)$. Since $\text{PGL}(3, 11)$ is transitive on lines, the order of G_{L_i} is the order of $\text{PGL}(3, 11)$ divided by the number of lines, so

$$|G_{L_i}| = \frac{|\text{PGL}(3, 11)|}{133} = \frac{11^3(11^3 - 1)(11^2 - 1)}{133} = 1597200.$$

3.3 Arcs of size and degree 5

Now to move out of the line into the plane, if \mathcal{P}'_1 and \mathcal{P}'_2 are considered to be the two sets \mathcal{P}_1 and \mathcal{P}_2 on the line $L_0 \subset \text{PG}(2, 11)$ that is the line with equation $Z = 0$, namely the third coordinate of its points is 0. Then, the two distinct arcs of size and degree 5 are of type $[77, 55, 0, 0, 0, 1]$ and their points coordinates are the following:

$$\mathcal{P}'_1 = \{\mathbf{P}(1, 0, 0), \mathbf{P}(0, 1, 0), \mathbf{P}(1, 1, 0); \mathbf{P}(-1, 1, 0), \mathbf{P}(2, 1, 0)\}$$

$$\mathcal{P}'_2 = \{\mathbf{P}(1, 0, 0), \mathbf{P}(0, 1, 0), \mathbf{P}(1, 1, 0), \mathbf{P}(-2, 1, 0), \mathbf{P}(3, 1, 0)\}.$$

By normalising the \mathcal{P}'_1 and \mathcal{P}'_2 points we get the following:

$$\mathcal{P}'_1 = \{\mathbf{P}(1, 0, 0), \mathbf{P}(0, 1, 0), \mathbf{P}(1, 1, 0), \mathbf{P}(1, -1, 0), \mathbf{P}(1, -5, 0)\};$$

$$\mathcal{P}'_2 = \{\mathbf{P}(1, 0, 0), \mathbf{P}(0, 1, 0), \mathbf{P}(1, 1, 0), \mathbf{P}(1, 5, 0), \mathbf{P}(1, 4, 0)\}.$$

The group fixing \mathcal{P}'_1 under $\text{PGL}(3, 11)$ is the group

$$G(\mathcal{P}'_1) = \left\{ \begin{bmatrix} tA & & 0 \\ & a_{31} & a_{32} \\ & & 1 \end{bmatrix}, \text{ where } A \in \left\langle \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix} \right\rangle, t \in \mathbf{F}_{11} \setminus \{0\}, a_{31}, a_{32} \in \mathbf{F}_{11} \right\}$$

of order

$$\left|G(\mathcal{P}'_1)\right|=(2)(11)(11)(10)=2,420.$$

Also,

$$G(\mathcal{P}'_2)=\left\{\begin{bmatrix} tA & 0 \\ a_{31} & a_{32} & 1 \end{bmatrix}, \text{ where } A \in \left\langle \begin{bmatrix} 0 & -2 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix} \right\rangle, t \in \mathbf{F}_{11} \setminus \{0\}, a_{31}, a_{32} \in \mathbf{F}_{11} \right\}$$

is the group of order

$$\left|G(\mathcal{P}'_2)\right|=(10)(11)(11)(10)=12,100$$

that stabilises \mathcal{P}'_2 . These stabiliser groups with their details are listed in Table 3.2.

Table 3.2: The projectively distinct $(5, 5)$ -arcs in $\text{PG}(2, 11)$

Notation	$ G $	Group generators
\mathcal{P}'_1	2420	M_1, M_2, \dots, M_6
\mathcal{P}'_2	12100	N_1, N_2, \dots, N_8

Here

$$M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 4 & 7 \end{pmatrix}, M_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 8 & 9 & 9 \end{pmatrix}, M_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 8 \end{pmatrix}, M_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix},$$

$$M_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}, M_6 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 7 & 2 & 4 \end{pmatrix}$$

and

$$N_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 6 & 3 & 10 \end{pmatrix}, N_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 8 & 4 & 5 \end{pmatrix}, N_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 7 & 1 \end{pmatrix}, N_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix},$$

$$N_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}, N_6 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix}, N_7 = \begin{pmatrix} 0 & 1 & 0 \\ 2 & 10 & 0 \\ 9 & 9 & 3 \end{pmatrix}, N_8 = \begin{pmatrix} 1 & 0 & 0 \\ 10 & 10 & 0 \\ 5 & 2 & 8 \end{pmatrix}$$

Theorem 3.3.1. *In $\text{PG}(2, 11)$, there are up to projective equivalence exactly two $(5, 5)$ -arcs of type $[77, 55, 0, 0, 0, 1]$ and different group order presented in Table 3.2.*

Note 3.3.2. The set of points

$$\{U_0 = \mathbf{P}(1, 0, 0), U_1 = \mathbf{P}(0, 1, 0), U_2 = \mathbf{P}(0, 0, 1), U = \mathbf{P}(1, 1, 1)\}$$

form the frame points in the projective plane $\text{PG}(2, q)$.

3.4 Arcs of size 6 and degree 5

By considering the action of the group of projectivities of \mathcal{P}'_1 and \mathcal{P}'_2 , those groups will have orbits on the points of $\text{PG}(2, 11)$ off the line L_0 where L_0 is the line with equation $Z = 0$ as it is the only 5-secant so far. That is the 121 points of the set C_0^5 of \mathcal{P}'_1 and \mathcal{P}'_2 . The projective groups operate transitively on the corresponding set C_0^5 , namely $\text{PG}(2, 11) \setminus L_0$. By suitably choosing a point from C_0^5 ($U_0 = \mathbf{P}(1, 0, 0)$ for convenience) and add it to the $(5, 5)$ -arcs \mathcal{P}'_1 and \mathcal{P}'_2 in Section 3.3. Therefore, there are two different classes of $(6, 5)$ -arcs of the same type with two different sizes of stabiliser groups. Their points coordinates are the following.

$$\mathcal{P}'_1 = \{\mathbf{P}(1, 0, 0), \mathbf{P}(0, 1, 0), \mathbf{P}(1, 1, 0), \mathbf{P}(1, -1, 0), \mathbf{P}(1, -5, 0), \mathbf{P}(0, 0, 1)\}$$

$$\mathcal{P}'_2 = \{\mathbf{P}(1, 0, 0), \mathbf{P}(0, 1, 0), \mathbf{P}(1, 1, 0), \mathbf{P}(1, 5, 0), \mathbf{P}(1, 4, 0), \mathbf{P}(0, 0, 1)\}$$

Theorem 3.4.1. *In $\text{PG}(2, 11)$, there are up to projective equivalence exactly two $(6, 5)$ -arcs of type $[70, 57, 5, 0, 0, 1]$ and different groups presented in Table 3.3.*

3.5 Arcs of size 7 and degree 5

The set C_0^6 of 120 points corresponding to \mathcal{P}'_1 is split into 7 orbits of orders 10, 20, 10, 20, 20, 20, 20 under the action of the group $C_{10} \times C_2$. The points of the first, second, and sixth orbit

Table 3.3: The projectively distinct $(6, 5)$ -arcs in $\text{PG}(2, 11)$

Notation	G	$ G $	Group generators		
\mathcal{P}'_1	$C_{10} \times C_2$	20	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 9 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 7 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 10 & 10 & 0 \\ 0 & 0 & 6 \end{pmatrix}$
\mathcal{P}'_2	$C_{10} \rtimes D_{10}$	100	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 6 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 8 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 0 \\ 2 & 10 & 0 \\ 0 & 0 & 5 \end{pmatrix}$ $\begin{pmatrix} 1 & 0 & 0 \\ 10 & 10 & 0 \\ 0 & 0 & 3 \end{pmatrix}$

are of type $[7, 4, 1, 0, 0, 0]$ while the other orbits points are of type $[6, 6, 0, 0, 0, 0]$. This gives 7 different classes of $(7, 5)$ -arcs of \mathcal{P}'_1 , $\{\mathcal{P}'_1^{(i)} \mid i = 1, 2, \dots, 7\}$ of two different types $[63, 60, 8, 1, 0, 1]$ and $[64, 57, 11, 0, 0, 1]$, and two different group orders as shown in Table 3.4.

The action of $C_{10} \rtimes D_{10}$, the group of \mathcal{P}'_2 , splits the 120 points of the set C_0^6 of \mathcal{P}'_2 into 3 orbits of order 50, 50, 20. The first orbit points are of type $[7, 4, 1, 0, 0, 0]$ and the remaining orbits points are of type $[6, 6, 0, 0, 0, 0]$. So, extending \mathcal{P}'_2 gives another three different classes of $(7, 5)$ -arcs with two different types $[63, 60, 8, 1, 0, 1]$ and $[64, 57, 11, 0, 0, 1]$, and two different group orders. All details are in Table 3.4.

Theorem 3.5.1. *In $\text{PG}(2, 11)$, there are exactly 10 projectively distinct $(7, 5)$ -arcs.*

 Table 3.4: The projectively distinct $(7, 5)$ -arcs in $\text{PG}(2, 11)$

Notation	Arc	G	$ G $	Group generators
$\mathcal{P}'_1^{(1)}$	$\{1, 2, 3, 4, 9, 13, 16\}$	$C_2 \times C_2$	4	$\begin{pmatrix} 1 & 0 & 0 \\ 10 & 10 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 10 & 0 & 10 \end{pmatrix}$
$\mathcal{P}'_1^{(2)}$	$\{1, 2, 3, 6, 8, 13, 16\}$	C_2	2	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 10 & 10 \end{pmatrix}$

$\mathcal{P}_1'^{(3)}$	$\{1, 2, 5, 7, 8, 13, 16\}$	$C_2 \times C_2$	4	$\begin{pmatrix} 1 & 0 & 0 \\ 10 & 10 & 0 \\ 1 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 10 & 9 & 10 \end{pmatrix}$
$\mathcal{P}_1'^{(4)}$	$\{1, 2, 4, 6, 9, 13, 16\}$	C_2	2	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 10 & 8 & 10 \end{pmatrix}$
$\mathcal{P}_1'^{(5)}$	$\{1, 2, 5, 9, 10, 13, 16\}$	C_2	2	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 10 & 7 & 10 \end{pmatrix}$
$\mathcal{P}_1'^{(6)}$	$\{1, 2, 3, 4, 11, 13, 16\}$	C_2	2	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 10 & 5 & 10 \end{pmatrix}$
$\mathcal{P}_1'^{(7)}$	$\{1, 2, 6, 9, 11, 13, 16\}$	C_2	2	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 10 & 3 & 10 \end{pmatrix}$
$\mathcal{P}_2'^{(1)}$	$\{1, 2, 3, 10, 11, 13, 16\}$	$C_2 \times C_2$	4	$\begin{pmatrix} 1 & 0 & 0 \\ 10 & 10 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 10 & 0 & 10 \end{pmatrix}$
$\mathcal{P}_2'^{(2)}$	$\{1, 2, 4, 8, 10, 13, 16\}$	$C_2 \times C_2$	4	$\begin{pmatrix} 1 & 0 & 0 \\ 10 & 10 & 0 \\ 1 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 10 & 9 & 10 \end{pmatrix}$
$\mathcal{P}_2'^{(3)}$	$\{1, 2, 4, 10, 12, 13, 16\}$	C_{10}	4	$\begin{pmatrix} 0 & 1 & 0 \\ 2 & 10 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 10 & 5 & 10 \end{pmatrix}$

Remark 3.5.2. The 10 projectively distinct arcs in Table 3.4 are transformed into the projectively equivalent ones that include the standard frame in Definition 2.4.5. From now on, we will use numbers, indices, to indicate points of arcs instead of their coordinates where each point is represented uniquely by number from the set $\{1, 2, \dots, 133\}$. These numbers represent the position of each point in $\text{PG}(2, 11)$ as given to it in the FinInG package [6]. Also, The FinInG package labelling of the standard frame points is $\{1, 2, 13, 16\}$ respectively.

3.6 Arcs of size 8 and degree 5

The action of the stabiliser group of each distinct $(7, 5)$ -arc on the corresponding set C_0^7 splits this set into 456 orbits of different orders and their points have also different point types. All the orbits and their points details are shown in Table 3.5, where the cell $n : m$ means that n is the number of orbits that have order m . As Table 3.6 indicates, the action of the automorphism subgroup under $\text{PGL}(3, 11)$ on the remaining points gives rise to 127 arcs with a trivial stabiliser group, 29 arcs with group C_2 , four with $C_2 \times C_2$, one arc with group C_{10} and another one with stabiliser C_5 .

Theorem 3.6.1. *Up to projective equivalence, there are exactly 162 arcs of size 8 and degree 5 in $\text{PG}(2, 11)$.*

Table 3.5: The orbits and points types of $(8, 5)$ -arcs in $\text{PG}(2, 11)$

Arc	No. of orbits	$ Orbit $	$n : m$	points type
$\mathcal{P}_1'^{(1)}$	35	1	1 : 1	$[8, 3, 0, 1, 0, 0]$
			1 : 2	$[8, 2, 2, 0, 0, 0]$
			1 : 2	$[7, 4, 1, 0, 0, 0]$
		2	4 : 2	$[8, 3, 0, 1, 0, 0]$
			3 : 2	$[6, 6, 0, 0, 0, 0]$
			1 : 4	$[8, 2, 2, 0, 0, 0]$
		4	10 : 4	$[7, 4, 1, 0, 0, 0]$
			14 : 4	$[6, 6, 0, 0, 0, 0]$

$\mathcal{P}'^{(2)}_1$	60	1	1 : 1	[8, 3, 0, 1, 0, 0]
			3 : 2	[8, 2, 2, 0, 0, 0]
			24 : 2	[7, 4, 1, 0, 0, 0]
			4 : 2	[8, 3, 0, 1, 0, 0]
			28 : 2	[6, 6, 0, 0, 0, 0]
$\mathcal{P}'^{(3)}_1$	35	1	1 : 1	[7, 4, 1, 0, 0, 0]
			1 : 2	[8, 2, 2, 0, 0, 0]
			5 : 2	[7, 4, 1, 0, 0, 0]
		2	3 : 2	[6, 6, 0, 0, 0, 0]
			4 : 4	[8, 2, 2, 0, 0, 0]
			15 : 4	[7, 4, 1, 0, 0, 0]
$\mathcal{P}'^{(4)}_1$	60	1	1 : 1	[7, 4, 1, 0, 0, 0]
			6 : 2	[8, 2, 2, 0, 0, 0]
		2	32 : 2	[7, 4, 1, 0, 0, 0]
			21 : 2	[6, 6, 0, 0, 0, 0]
$\mathcal{P}'^{(5)}_1$	60	1	1 : 1	[8, 3, 1, 0, 0, 0]
			28 : 2	[8, 3, 1, 0, 0, 0]
		2	28 : 2	[7, 5, 0, 0, 0, 0]
			3 : 2	[9, 1, 2, 0, 0, 0]
$\mathcal{P}'^{(6)}_1$	60	1	1 : 1	[8, 3, 0, 1, 0, 0]
			3 : 2	[8, 2, 2, 0, 0, 0]
			24 : 2	[7, 4, 1, 0, 0, 0]
		2	4 : 2	[8, 3, 0, 1, 0, 0]
			28 : 2	[6, 6, 0, 0, 0, 0]
$\mathcal{P}'^{(7)}_1$	60	1	1 : 1	[8, 3, 1, 0, 0, 0]
			28 : 2	[8, 3, 1, 0, 0, 0]
		2	28 : 2	[7, 5, 0, 0, 0, 0]
			3 : 2	[9, 1, 2, 0, 0, 0]

$\mathcal{P}_2'^{(1)}$	35	1	1 : 1	[9, 2, 0, 1, 0, 0]
			2 : 2	[8, 3, 1, 0, 0, 0]
		2	4 : 2	[9, 2, 0, 1, 0, 0]
			3 : 2	[7, 5, 0, 0, 0, 0]
			13 : 4	[8, 3, 1, 0, 0, 0]
		4	1 : 4	[9, 1, 2, 0, 0, 0]
			11 : 4	[7, 5, 0, 0, 0, 0]
$\mathcal{P}_2'^{(2)}$	35	1	1 : 1	[8, 3, 1, 0, 0, 0]
			6 : 2	[8, 3, 1, 0, 0, 0]
		2	3 : 2	[7, 5, 0, 0, 0, 0]
			12 : 4	[8, 3, 1, 0, 0, 0]
		4	3 : 4	[9, 1, 2, 0, 0, 0]
			8 : 4	[7, 5, 0, 0, 0, 0]
$\mathcal{P}_2'^{(3)}$	16	1	1 : 1	[8, 3, 1, 0, 0, 0]
		2	4 : 2	[8, 3, 1, 0, 0, 0]
		10	6 : 10	[8, 3, 1, 0, 0, 0]
			3 : 10	[7, 5, 0, 0, 0, 0]
			2 : 10	[9, 1, 2, 0, 0, 0]

Table 3.6: The projectively distinct $(8, 5)$ -arcs in $\text{PG}(2, 11)$

No. of $(8, 5)$ -arcs	G
1	C_5
1	C_{10}
4	$C_2 \times C_2$
29	C_2
127	$\mathbf{1}_G$

Table 3.7: Orbits of $(8, 5)$ -arcs and their order

No. of orbits	Orbit order	No. of orbits	Orbit order
1	15	5	59
1	30	20	64
4	34	127	118
4	63		

3.7 Arcs of size 9 and degree 5

Theorem 3.7.1. *In $\text{PG}(2, 11)$, there are exactly 4,404 projectively distinct $(9, 5)$ -arcs.*

Table 3.8: The projectively distinct $(9, 5)$ -arcs in $\text{PG}(2, 11)$

No. of arcs	Arcs type	G	$ G $
1	[49, 66, 16, 0, 0, 2]	$\mathbf{1}_G$	1
6	[49, 66, 16, 0, 0, 2]	C_2	2
1	[49, 66, 16, 0, 0, 2]	$C_2 \times C_2$	4
2	[49, 66, 16, 0, 0, 2]	D_8	8
12	[49, 68, 11, 3, 1, 1]	$\mathbf{1}_G$	1
12	[49, 69, 8, 6, 0, 1]	C_2	2
124	[50, 65, 14, 2, 1, 1]	$\mathbf{1}_G$	1
4	[50, 65, 14, 2, 1, 1]	C_2	2
40	[50, 66, 11, 5, 0, 1]	$\mathbf{1}_G$	1
20	[50, 66, 11, 5, 0, 1]	C_2	2
4	[50, 66, 11, 5, 0, 1]	C_2	2
252	[51, 62, 17, 1, 1, 1]	$\mathbf{1}_G$	1
406	[51, 63, 14, 4, 0, 1]	$\mathbf{1}_G$	1
44	[51, 63, 14, 4, 0, 1]	C_2	2
4	[51, 63, 14, 4, 0, 1]	$C_2 \times C_2$	4
108	[52, 59, 20, 0, 1, 1]	$\mathbf{1}_G$	1
2	[52, 59, 20, 0, 1, 1]	C_{10}	10
2	[52, 59, 20, 0, 1, 1]	C_{10}	10

16	[52, 59, 20, 0, 1, 1]	C_2	2
4	[52, 59, 20, 0, 1, 1]	$C_2 \times C_2$	4
2	[52, 59, 20, 0, 1, 1]	C_5	5
1, 252	[52, 60, 17, 3, 0, 1]	$\mathbf{1}_G$	5
104	[52, 60, 17, 3, 0, 1]	C_2	2
1, 348	[53, 57, 20, 2, 0, 1]	$\mathbf{1}_G$	1
70	[53, 57, 20, 2, 0, 1]	C_2	2
6	[53, 57, 20, 2, 0, 1]	$C_2 \times C_2$	4
452	[54, 54, 23, 1, 0, 1]	$\mathbf{1}_G$	1
56	[54, 54, 23, 1, 0, 1]	C_2	2
6	[54, 54, 23, 1, 0, 1]	C_2	2
34	[55, 51, 26, 0, 0, 1]	$\mathbf{1}_G$	1
20	[55, 51, 26, 0, 0, 1]	C_2	2

3.8 Arcs of size 10 and degree 5

Theorem 3.8.1. *In $\text{PG}(2, 11)$, there are exactly 98,645 projectively distinct $(10, 5)$ -arcs.*

Table 3.9: The projectively distinct $(10, 5)$ -arcs in $\text{PG}(2, 11)$

No. of arcs	Arcs type	G	$ G $
2	[42, 72, 13, 4, 0, 2]	$C_2 \times C_2$	4
6	[42, 73, 11, 4, 2, 1]	C_2	2
1	[42, 74, 8, 7, 1, 1]	C_2	2
1	[42, 75, 5, 10, 0, 1]	D_{10}	10
40	[43, 69, 16, 3, 0, 2]	$\mathbf{1}_G$	1
4	[43, 69, 16, 3, 0, 2]	C_2	2
60	[43, 70, 14, 3, 2, 1]	$\mathbf{1}_G$	1
37	[43, 71, 11, 6, 1, 1]	$\mathbf{1}_G$	1

No. of arcs	Arcs type	G	$ G $
4	[43, 71, 11, 6, 1, 1]	C_2	2
1	[43, 72, 8, 9, 0, 1]	$\mathbf{1}_G$	1
180	[44, 66, 19, 2, 0, 2]	$\mathbf{1}_G$	1
18	[44, 66, 19, 2, 0, 2]	C_2	2
336	[44, 67, 17, 2, 2, 1]	$\mathbf{1}_G$	1
28	[44, 67, 17, 2, 2, 1]	C_2	2
4	[44, 67, 17, 2, 2, 1]	$C_2 \times C_2$	4
593	[44, 68, 14, 5, 1, 1]	$\mathbf{1}_G$	1
33	[44, 68, 14, 5, 1, 1]	C_2	2
4	[44, 68, 14, 5, 1, 1]	$C_2 \times C_2$	4
45	[44, 69, 11, 8, 0, 1]	$\mathbf{1}_G$	1
17	[44, 69, 11, 8, 0, 1]	C_2	2
206	[45, 63, 22, 1, 0, 2]	$\mathbf{1}_G$	1
8	[45, 63, 22, 1, 0, 2]	C_2	2
564	[45, 64, 20, 1, 2, 1]	$\mathbf{1}_G$	1
3, 706	[45, 65, 17, 4, 1, 1]	$\mathbf{1}_G$	1
38	[45, 65, 17, 4, 1, 1]	C_2	2
876	[45, 66, 14, 7, 0, 1]	$\mathbf{1}_G$	1
2	[45, 66, 14, 7, 0, 1]	C_2	2
50	[46, 60, 25, 0, 0, 2]	$\mathbf{1}_G$	1
2	[46, 60, 25, 0, 0, 2]	C_{10}	10
20	[46, 60, 25, 0, 0, 2]	C_2	2
1	[46, 60, 25, 0, 0, 2]	$C_2 \times C_2$	4
3	[46, 60, 25, 0, 0, 2]	C_5	5
1	[46, 60, 25, 0, 0, 2]	$C_5 \times D_{10}$	50
2	[46, 60, 25, 0, 0, 2]	D_8	8
224	[46, 61, 23, 0, 2, 1]	$\mathbf{1}_G$	1
26	[46, 61, 23, 0, 2, 1]	C_2	2

No. of arcs	Arcs type	G	$ G $
9, 170	[46, 62, 20, 3, 1, 1]	$\mathbf{1}_G$	1
131	[46, 62, 20, 3, 1, 1]	C_2	2
6, 054	[46, 63, 17, 6, 0, 1]	$\mathbf{1}_G$	1
165	[46, 62, 20, 6, 1, 1]	C_2	2
8, 853	[47, 59, 23, 2, 1, 1]	$\mathbf{1}_G$	1
72	[47, 59, 23, 2, 1, 1]	C_2	2
18, 759	[47, 60, 20, 5, 0, 1]	$\mathbf{1}_G$	1
18	[47, 60, 20, 5, 0, 1]	C_2	2
2	[47, 60, 20, 5, 0, 1]	C_5	5
3, 103	[48, 56, 26, 1, 1, 1]	$\mathbf{1}_G$	1
65	[48, 56, 26, 1, 1, 1]	C_2	2
6	[48, 56, 26, 1, 1, 1]	$C_2 \times C_2$	4
25, 267	[48, 57, 23, 4, 0, 1]	$\mathbf{1}_G$	1
279	[48, 57, 23, 4, 0, 1]	C_2	1
6	[48, 57, 23, 4, 0, 1]	$C_2 \times C_2$	4
284	[49, 53, 29, 0, 1, 1]	$\mathbf{1}_G$	1
26	[49, 53, 29, 0, 1, 1]	C_2	2
14, 970	[49, 54, 26, 3, 0, 1]	$\mathbf{1}_G$	1
24	[49, 54, 26, 3, 0, 1]	C_2	2
3, 746	[50, 51, 29, 2, 0, 1]	$\mathbf{1}_G$	1
118	[50, 51, 29, 2, 0, 1]	C_2	2
360	[51, 48, 32, 1, 0, 1]	$\mathbf{1}_G$	1
6	[51, 48, 32, 1, 0, 1]	C_2	1
8	[52, 45, 35, 0, 0, 1]	$\mathbf{1}_G$	1
7	[52, 45, 35, 0, 0, 1]	C_2	2
1	[52, 45, 35, 0, 0, 1]	D_{10}	10

Chapter 4

Results for arcs of degree 5 and length at most 13

Arcs of length up to 10 can be computed just using a sequential version of the code within an hour on an ordinary laptop. For large arcs the complexity of calculations grows exponentially so that parallel calculations are needed in this stage. The current parallel calculation set-up requires one master process, that uses large amount of memory to store all currently known arcs, and multiple workers, slaves, with moderate amount of memory. Parallelising the calculation has been implemented using a GAP package called SCSCP [26]. we used the GAP package SCSCP, which implements the remote procedure call protocol with the same name (the abbreviation SCSCP stands for "Symbolic Computation Software Composability

4.1 The GAP SCSCP package

To run GAP in parallel, we used the GAP package SCSCP [26], which implements the remote procedure call protocol with the same name (the abbreviation SCSCP stands for "Symbolic Computation Software Composability protocol". This protocol uses OpenMath encoding both for protocol instructions and for the mathematical objects transmitted between several copies of GAP (and, if necessary, other compliant software) running locally or remotely. The SCSCP protocol consists of

1. SCSCP server;

2. SCSCP client.

Although there are several approaches to initiate a GAP ScScP server, the way we exploit it is by using a shell script `gapd.sh`, which triggers GAP to operate as a daemon. A daemon is a unix term for a program that runs in the background. The ScScP server communicates with ScScP client/s through a designated port number specified by the Internet Assigned Numbers Authority (IANA). It then assigns tasks to these clients (workers) and next listens to that port to collect the resulted outcomes. The SCSCP package implements a master-worker parallel computation skeleton: a GAP master (SCSCP client) concurrently sends portions of work to a number of GAP workers (SCSCP servers),

which receive the work assignments through a designated port number specified by the Internet Assigned Numbers Authority (IANA). The worker jobs then perform the actual jobs that they are assigned to.

4.2 The projectively distinct $(11, 5)$ -arcs

The distributed calculation of $(11, 5)$ -arcs took 2 hours and 37 minutes. This calculation was started with 48 workers on the computational cluster of the Centre for Interdisciplinary Research in Computational Algebra at the University of St Andrews. All details of the $(11, 5)$ -arcs that have been established in this stage are summarised in Table 4.1.

Theorem 4.2.1. *In $\text{PG}(2, 11)$, there are exactly 1,880,729 projectively distinct $(11, 5)$ -arcs.*

Table 4.1: The projectively distinct $(11, 5)$ -arcs in $\text{PG}(2, 11)$

No. of arcs	Arc type	G	$ G $
4	$[36, 75, 14, 5, 1, 2]$	$\mathbf{1}_G$	1
4	$[36, 75, 14, 5, 1, 2]$	C_2	2
2	$[36, 75, 15, 2, 4, 1]$	C_2	2
1	$[36, 76, 11, 8, 0, 2]$	C_2	2

No. of arcs	Arc type	G	$ G $
2	[36, 76, 11, 8, 0, 2]	D_8	8
5	[36, 76, 12, 5, 3, 1]	$\mathbf{1}_G$	1
2	[36, 76, 12, 5, 3, 1]	C_2	2
1	[36, 77, 9, 8, 2, 1]	$\mathbf{1}_G$	1
3	[36, 77, 9, 8, 2, 1]	C_2	2
94	[36, 72, 17, 4, 1, 2]	$\mathbf{1}_G$	1
4	[37, 72, 18, 1, 4, 1]	C_2	2
2	[37, 72, 18, 1, 4, 1]	C_2	2
20	[37, 73, 14, 7, 0, 2]	$\mathbf{1}_G$	1
11	[37, 73, 14, 7, 0, 2]	C_2	2
1	[37, 73, 14, 7, 0, 2]	$C_2 \times C_2$	4
88	[37, 73, 15, 4, 3, 1]	$\mathbf{1}_G$	1
50	[37, 74, 12, 7, 2, 1]	$\mathbf{1}_G$	1
14	[37, 74, 12, 7, 2, 1]	C_2	2
3	[37, 75, 9, 10, 1, 1]	$\mathbf{1}_G$	1
1	[37, 76, 6, 13, 0, 1]	$C_2 \times C_2$	4
596	[38, 69, 20, 3, 1, 2]	$\mathbf{1}_G$	1
8	[38, 69, 20, 3, 1, 2]	C_2	2
16	[38, 69, 21, 0, 4, 1]	$\mathbf{1}_G$	1
414	[38, 70, 17, 6, 0, 2]	$\mathbf{1}_G$	1
62	[38, 70, 17, 6, 0, 2]	C_2	2
586	[38, 70, 18, 3, 3, 1]	$\mathbf{1}_G$	1
16	[38, 70, 18, 3, 3, 1]	C_2	2
1, 122	[38, 71, 15, 6, 2, 1]	$\mathbf{1}_G$	1
51	[38, 71, 15, 6, 2, 1]	C_2	2
1	[38, 71, 15, 6, 2, 1]	$C_2 \times C_2$	4
160	[38, 72, 12, 9, 1, 1]	$\mathbf{1}_G$	1
7	[38, 72, 12, 9, 1, 1]	C_2	2

No. of arcs	Arc type	G	$ G $
2	[38, 72, 12, 9, 1, 1]	$C_2 \times C_2$	4
2	[38, 73, 9, 12, 0, 1]	$C_2 \times C_2$	4
1	[38, 73, 9, 12, 0, 1]	$C_2 \times C_2$	4
1, 296	[39, 66, 23, 2, 1, 2]	$\mathbf{1}_G$	1
24	[39, 66, 23, 2, 1, 2]	C_2	2
2, 658	[39, 67, 20, 5, 0, 2]	$\mathbf{1}_G$	1
1	[39, 67, 20, 5, 0, 2]	C_{10}	10
90	[39, 67, 20, 5, 0, 2]	C_2	2
5	[39, 67, 20, 5, 0, 2]	$C_2 \times C_2$	4
1, 604	[39, 67, 21, 2, 3, 1]	$\mathbf{1}_G$	1
8, 707	[39, 68, 18, 5, 2, 1]	$\mathbf{1}_G$	1
120	[39, 68, 18, 5, 2, 1]	C_2	2
3, 193	[39, 69, 15, 8, 1, 1]	$\mathbf{1}_G$	1
7	[39, 69, 15, 8, 1, 1]	C_2	2
94	[39, 70, 12, 11, 0, 1]	$\mathbf{1}_G$	1
25	[39, 70, 12, 11, 0, 1]	C_2	2
4	[39, 70, 12, 11, 0, 1]	$C_2 \times C_2$	4
1, 002	[40, 63, 26, 1, 1, 2]	$\mathbf{1}_G$	1
7, 372	[40, 64, 23, 4, 0, 2]	$\mathbf{1}_G$	1
187	[40, 64, 23, 4, 0, 2]	C_2	2
8	[40, 64, 23, 4, 0, 2]	$C_2 \times C_2$	4
2	[40, 64, 23, 4, 0, 2]	C_4	4
1, 597	[40, 64, 24, 1, 3, 1]	$\mathbf{1}_G$	1
18	[40, 64, 24, 1, 3, 1]	C_2	2
30, 438	[40, 65, 21, 4, 2, 1]	$\mathbf{1}_G$	1
270	[40, 65, 21, 4, 2, 1]	C_2	2
3	[40, 65, 21, 4, 2, 1]	$C_2 \times C_2$	4
28, 903	[40, 66, 18, 7, 1, 1]	$\mathbf{1}_G$	1

No. of arcs	Arc type	G	$ G $
139	[40, 66, 18, 7, 1, 1]	C_2	2
2, 377	[40, 67, 15, 10, 0, 1]	$\mathbf{1}_G$	1
103	[40, 67, 15, 10, 0, 1]	C_2	2
3	[40, 67, 15, 10, 0, 1]	$C_2 \times C_2$	4
1	[40, 67, 15, 10, 0, 1]	C_5	5
1	[40, 67, 15, 10, 0, 1]	D_{10}	10
218	[41, 60, 29, 0, 1, 2]	$\mathbf{1}_G$	1
20	[41, 60, 29, 0, 1, 2]	C_2	2
8, 686	[41, 61, 26, 3, 0, 2]	$\mathbf{1}_G$	1
141	[41, 61, 26, 3, 0, 2]	C_2	2
3	[41, 61, 26, 3, 0, 2]	$C_2 \times C_2$	2
380	[41, 61, 27, 0, 3, 1]	$\mathbf{1}_G$	1
48, 534	[41, 62, 24, 3, 2, 1]	$\mathbf{1}_G$	1
242	[41, 62, 24, 3, 2, 1]	C_2	2
121, 322	[41, 63, 21, 6, 1, 1]	$\mathbf{1}_G$	1
78	[41, 63, 21, 6, 1, 1]	C_2	2
23, 589	[41, 64, 18, 9, 0, 1]	$\mathbf{1}_G$	1
326	[41, 64, 18, 9, 0, 1]	C_2	2
12	[41, 64, 18, 9, 0, 1]	$C_2 \times C_2$	2
4, 318	[42, 58, 29, 2, 2, 1]	$\mathbf{1}_G$	1
172	[42, 58, 29, 2, 2, 1]	C_2	2
33, 256	[42, 59, 27, 2, 2, 1]	$\mathbf{1}_G$	1
231	[42, 59, 27, 2, 2, 1]	C_2	2
3	[42, 59, 27, 2, 2, 1]	$C_2 \times C_2$	4
244, 102	[42, 59, 27, 2, 2, 1]	$\mathbf{1}_G$	1
403	[42, 60, 24, 5, 1, 1]	C_2	2
12	[42, 60, 24, 5, 1, 1]	$C_2 \times C_2$	4
112, 950	[42, 61, 21, 8, 0, 1]	$\mathbf{1}_G$	4

No. of arcs	Arc type	G	$ G $
795	[42, 61, 21, 8, 0, 1]	C_2	2
9	[42, 61, 21, 8, 0, 1]	$C_2 \times C_2$	4
837	[43, 55, 32, 1, 0, 2]	$\mathbf{1}_G$	1
41	[43, 55, 32, 1, 0, 2]	C_2	2
3	[43, 55, 32, 1, 0, 2]	$C_2 \times C_2$	4
8, 845	[43, 56, 30, 1, 2, 1]	$\mathbf{1}_G$	1
76	[43, 56, 30, 1, 2, 1]	C_2	2
235, 176	[43, 57, 27, 4, 1, 1]	$\mathbf{1}_G$	1
168	[43, 57, 27, 4, 1, 1]	C_2	2
261, 859	[43, 58, 24, 7, 0, 1]	$\mathbf{1}_G$	1
1, 052	[43, 58, 24, 7, 0, 1]	C_2	2
18	[43, 58, 24, 7, 0, 1]	$C_2 \times C_2$	2
31	[44, 52, 35, 0, 0, 2]	$\mathbf{1}_G$	1
1	[44, 52, 35, 0, 0, 2]	C_{10}	10
23	[44, 52, 35, 0, 0, 2]	C_2	2
5	[44, 52, 35, 0, 0, 2]	$C_2 \times C_2$	2
2	[44, 52, 35, 0, 0, 2]	C_4	4
733	[44, 53, 33, 0, 2, 1]	$\mathbf{1}_G$	1
45	[44, 53, 33, 0, 2, 1]	C_2	2
3	[44, 53, 33, 0, 2, 1]	$C_2 \times C_2$	4
106, 071	[44, 54, 30, 3, 1, 1]	$\mathbf{1}_G$	1
307	[44, 54, 30, 3, 1, 1]	C_2	2
305, 733	[44, 55, 27, 6, 0, 1]	$\mathbf{1}_G$	1
1, 273	[44, 55, 27, 6, 0, 1]	C_2	2
15	[44, 55, 27, 6, 0, 1]	$C_2 \times C_2$	4
21, 575	[45, 51, 33, 2, 1, 1]	$\mathbf{1}_G$	1
90	[45, 51, 33, 2, 1, 1]	C_2	2
179, 034	[45, 52, 30, 5, 0, 1]	$\mathbf{1}_G$	1

No. of arcs	Arc type	G	$ G $
903	[45, 52, 30, 5, 0, 1]	C_2	2
9	[45, 52, 30, 5, 0, 1]	$C_2 \times C_2$	4
1	[45, 52, 30, 5, 0, 1]	C_5	5
1	[45, 52, 30, 5, 0, 1]	D_{10}	10
1, 720	[46, 48, 36, 1, 1, 1]	$\mathbf{1}_G$	1
38	[46, 48, 36, 1, 1, 1]	C_2	2
6	[46, 48, 36, 1, 1, 1]	$C_2 \times C_2$	4
52, 854	[46, 49, 33, 4, 0, 1]	$\mathbf{1}_G$	1
540	[46, 49, 33, 4, 0, 1]	C_2	2
6	[46, 49, 33, 4, 0, 1]	$C_2 \times C_2$	4
35	[47, 45, 39, 0, 1, 1]	$\mathbf{1}_G$	1
9	[47, 45, 39, 0, 1, 1]	C_2	2
7, 425	[47, 46, 36, 3, 0, 1]	$\mathbf{1}_G$	1
183	[47, 46, 36, 3, 0, 1]	C_2	2
6	[47, 46, 36, 3, 0, 1]	$C_2 \times C_2$	4
485	[48, 43, 39, 2, 0, 1]	$\mathbf{1}_G$	1
53	[48, 43, 39, 2, 0, 1]	C_2	2
6	[48, 43, 39, 2, 0, 1]	$C_2 \times C_2$	4
10	[49, 40, 42, 1, 0, 1]	$\mathbf{1}_G$	1
6	[49, 40, 42, 1, 0, 1]	C_2	2
1	[50, 37, 45, 0, 0, 1]	C_2	2

4.3 The projectively distinct $(12, 5)$ –arcs

The calculation of $(12, 5)$ -arcs took 20 hours to produce the result in a file of size 1,500 MB = 1.5 GB on two 64–core machines with 512 GB RAM each, available at St Andrews.

Theorem 4.3.1. *In $\text{PG}(2, 11)$, there are exactly 30,221,738 projectively distinct $(12, 5)$ –arcs.*

Table 4.2: Projectively inequivalent $(12, 5)$ -arcs in $\text{PG}(2, 11)$

No. of arcs	Arc type	G	$ G $	No. of arcs	Arc type	G	$ G $
4	[30, 78, 15, 7, 0, 3]	\mathbf{S}_3	6	1	[30, 78, 16, 4, 3, 2]	\mathbf{I}_G	1
2	[30, 78, 16, 4, 3, 2]	C_2	2	1	[30, 79, 13, 7, 2, 2]	\mathbf{I}_G	1
3	[30, 79, 13, 7, 2, 2]	C_2	2	1	[30, 79, 13, 7, 2, 2]	$C_2 \times C_2$	4
4	[30, 79, 14, 4, 5, 1]	C_2	2	1	[30, 80, 10, 10, 1, 2]	C_2	2
1	[30, 80, 10, 10, 1, 2]	$C_2 \times C_2$	4	1	[30, 80, 11, 7, 4, 1]	$\mathbf{1}_G$	1
4	[30, 80, 11, 7, 4, 1]	C_2	2	1	[30, 81, 8, 10, 3, 1]	$C_2 \times C_2$	4
8	[31, 75, 18, 6, 0, 3]	$\mathbf{1}_G$	1	10	[31, 75, 18, 6, 0, 3]	C_3	3
16	[31, 75, 19, 3, 3, 2]	$\mathbf{1}_G$	1	1	[31, 75, 19, 3, 3, 2]	C_2	2
56	[31, 76, 16, 6, 2, 2]	$\mathbf{1}_G$	1	9	[31, 76, 17, 3, 5, 1]	$\mathbf{1}_G$	1
1	[31, 76, 17, 3, 5, 1]	C_2	2	9	[31, 77, 13, 9, 1, 2]	$\mathbf{1}_G$	1
2	[31, 77, 13, 9, 1, 2]	C_2	2	39	[31, 77, 14, 6, 4, 1]	$\mathbf{1}_G$	1
9	[31, 78, 11, 9, 3, 1]	$\mathbf{1}_G$	1	94	[32, 72, 21, 5, 0, 3]	$\mathbf{1}_G$	1
24	[32, 72, 21, 5, 0, 3]	C_2	2	85	[32, 72, 22, 2, 3, 2]	$\mathbf{1}_G$	1
652	[32, 73, 19, 5, 2, 2]	$\mathbf{1}_G$	1	27	[32, 73, 19, 5, 2, 2]	C_2	2
41	[32, 73, 20, 2, 5, 1]	$\mathbf{1}_G$	1	17	[32, 73, 20, 2, 5, 1]	C_2	2
354	[32, 74, 16, 8, 1, 2]	$\mathbf{1}_G$	1	34	[32, 74, 16, 8, 1, 2]	C_2	2
3	[32, 74, 16, 8, 1, 2]	$C_2 \times C_2$	4	2	[32, 74, 16, 8, 1, 2]	D_8	8
447	[32, 74, 17, 5, 4, 1]	$\mathbf{1}_G$	1	36	[32, 74, 17, 5, 4, 1]	C_2	2
1	[32, 74, 17, 5, 4, 1]	$C_2 \times C_2$	4	10	[32, 75, 13, 11, 0, 2]	$\mathbf{1}_G$	1
11	[32, 75, 13, 11, 0, 2]	C_2	2	317	[32, 75, 14, 8, 3, 1]	$\mathbf{1}_G$	1
40	[32, 75, 14, 8, 3, 1]	C_2	2	1	[32, 75, 14, 8, 3, 1]	$C_2 \times C_2$	4
19	[32, 76, 11, 11, 2, 1]	$\mathbf{1}_G$	1	15	[32, 76, 11, 11, 2, 1]	C_2	2
1	[32, 76, 11, 11, 2, 1]	$C_2 \times C_2$	4	1	[32, 77, 8, 14, 1, 1]	C_2	2
516	[33, 69, 24, 4, 0, 3]	$\mathbf{1}_G$	1	12	[33, 69, 24, 4, 0, 3]	C_2	2
8	[33, 69, 24, 4, 0, 3]	C_3	3	178	[33, 69, 25, 1, 3, 2]	$\mathbf{1}_G$	1

No. of arcs	Arc type	G	$ G $	No. of arcs	Arc type	G	$ G $
3	[33, 69, 25, 1, 3, 2]	C_2	2	3, 416	[33, 70, 22, 4, 2, 2]	$\mathbf{1}_G$	1
17	[33, 70, 22, 4, 2, 2]	C_2	2	73	[33, 70, 23, 1, 5, 1]	$\mathbf{1}_G$	1
3	[33, 70, 23, 1, 5, 1]	C_2	2	4, 390	[33, 71, 19, 7, 1, 2]	$\mathbf{1}_G$	1
48	[33, 71, 19, 7, 1, 2]	C_2	2	2, 965	[33, 71, 20, 4, 4, 1]	$\mathbf{1}_G$	1
6	[33, 71, 20, 4, 4, 1]	C_2	2	418	[33, 72, 16, 10, 0, 2]	$\mathbf{1}_G$	1
2	[33, 72, 16, 10, 0, 2]	C_{10}	10	3	[33, 72, 16, 10, 0, 2]	C_2	2
5, 177	[33, 72, 17, 7, 3, 1]	$\mathbf{1}_G$	1	18	[33, 72, 17, 7, 3, 1]	C_2	2
1, 064	[33, 73, 14, 10, 2, 1]	$\mathbf{1}_G$	1	8	[33, 73, 14, 10, 2, 1]	C_2	2
25	[33, 74, 11, 13, 1, 1]	$\mathbf{1}_G$	1	2	[33, 74, 11, 13, 1, 1]	C_2	2
972	[34, 66, 27, 3, 0, 3]	$\mathbf{1}_G$	1	20	[34, 66, 27, 3, 0, 3]	C_2	2
16	[34, 66, 27, 3, 0, 3]	C_3	3	88	[34, 66, 28, 3, 0, 2]	$\mathbf{1}_G$	1
19	[34, 66, 28, 3, 0, 2]	C_2	2	8, 157	[34, 67, 25, 3, 2, 2]	$\mathbf{1}_G$	1
69	[34, 67, 25, 3, 2, 2]	C_2	2	3	[34, 67, 25, 3, 2, 2]	$C_2 \times C_2$	4
35	[34, 67, 26, 0, 5, 1]	$\mathbf{1}_G$	1	13	[34, 67, 26, 0, 5, 1]	C_2	2
26, 245	[34, 68, 22, 0, 1, 2]	$\mathbf{1}_G$	1	219	[34, 68, 22, 6, 1, 2]	C_2	2
3	[34, 68, 22, 6, 1, 2]	$C_2 \times C_2$	4	8, 013	[34, 68, 23, 3, 4, 1]	$\mathbf{1}_G$	1
104	[34, 68, 23, 3, 4, 1]	C_2	2	5, 855	[34, 69, 19, 9, 0, 2]	$\mathbf{1}_G$	1
133	[34, 69, 19, 9, 0, 2]	C_2	2	7	[34, 69, 19, 9, 0, 2]	$C_2 \times C_2$	4
38, 852	[34, 69, 20, 6, 3, 1]	$\mathbf{1}_G$	1	328	[34, 69, 20, 6, 3, 1]	C_2	2
9	[34, 69, 20, 6, 3, 1]	$C_2 \times C_2$	4	19, 766	[34, 70, 17, 9, 2, 1]	$\mathbf{1}_G$	1
243	[34, 70, 17, 9, 2, 12]	C_2	2	1, 455	[34, 71, 14, 12, 1, 1]	$\mathbf{1}_G$	1
72	[34, 71, 14, 12, 1, 1]	C_2	2	3	[34, 71, 14, 12, 1, 1]	$C_2 \times C_2$	4
9	[34, 72, 11, 15, 0, 1]	$\mathbf{1}_G$	1	9	[34, 72, 11, 15, 0, 1]	C_2	2
890	[35, 63, 30, 2, 0, 3]	$\mathbf{1}_G$	1	24	[35, 63, 30, 2, 0, 3]	C_2	2
8, 815	[35, 64, 28, 2, 2, 2]	$\mathbf{1}_G$	1	47	[35, 64, 28, 2, 2, 2]	C_2	2
75, 865	[35, 65, 25, 5, 1, 2]	$\mathbf{1}_G$	1	162	[35, 65, 25, 5, 1, 2]	C_2	2
10, 277	[35, 65, 26, 2, 4, 1]	$\mathbf{1}_G$	1	21	[35, 65, 26, 2, 4, 1]	C_2	2
38, 399	[35, 66, 22, 8, 0, 2]	$\mathbf{1}_G$	1	58	[34, 66, 22, 8, 0, 2]	C_2	2
1	[34, 66, 28, 3, 0, 2]	$C_2 \times C_2$	4	142, 370	[35, 66, 23, 5, 3, 1]	$\mathbf{1}_G$	1
96	[35, 66, 23, 5, 3, 1]	C_2	2	17, 1870	[35, 67, 20, 8, 2, 1]	$\mathbf{1}_G$	1
58	[35, 67, 20, 8, 2, 1]	C_2	2	28, 800	[35, 68, 17, 11, 1, 1]	$\mathbf{1}_G$	1
37	[35, 68, 17, 11, 1, 1]	C_2	2	601	[35, 69, 14, 14, 0, 1]	$\mathbf{1}_G$	1
1	[35, 69, 14, 14, 0, 1]	C_2	2	306	[36, 60, 33, 1, 0, 3]	$\mathbf{1}_G$	1

No. of arcs	Arc type	G	$ G $	No. of arcs	Arc type	G	$ G $
8	[36, 60, 33, 1, 0, 3]	C_3	3	3, 514	[36, 61, 31, 1, 2, 2]	$\mathbf{1}_G$	1
27	[36, 61, 31, 1, 2, 2]	C_2	2	109, 682	[36, 62, 28, 4, 1, 2]	$\mathbf{1}_G$	1
433	[36, 62, 28, 4, 1, 2]	C_2	2	11	[36, 62, 28, 4, 1, 2]	$C_2 \times C_2$	4
2	[36, 62, 28, 4, 1, 2]	C_4	4	5, 561	[36, 62, 29, 1, 4, 1]	$\mathbf{1}_G$	1
42	[36, 62, 29, 1, 4, 1]	C_2	2	3	[36, 62, 29, 1, 4, 1]	$C_2 \times C_2$	4
126, 613	[36, 63, 25, 7, 0, 2]	$\mathbf{1}_G$	1	511	[36, 63, 25, 7, 0, 2]	C_2	2
256, 606	[36, 63, 26, 4, 3, 1]	$\mathbf{1}_G$	1	725	[36, 63, 26, 4, 3, 1]	C_2	2
3	[36, 63, 26, 4, 3, 1]	$C_2 \times C_2$	4	742, 866	[36, 64, 23, 7, 2, 1]	$\mathbf{1}_G$	1
1, 093	[36, 64, 23, 7, 2, 1]	C_2	2	12	[36, 64, 23, 7, 2, 1]	$C_2 \times C_2$	4
275, 991	[36, 65, 20, 10, 1, 1]	$\mathbf{1}_G$	1	761	[36, 65, 20, 10, 1, 1]	C_2	2
3	[36, 65, 20, 10, 1, 1]	$C_2 \times C_2$	4	13, 650	[36, 66, 17, 13, 0, 1]	$\mathbf{1}_G$	1
264	[36, 66, 17, 13, 0, 1]	C_2	2	3	[36, 66, 17, 13, 0, 1]	$C_2 \times C_2$	4
30	[37, 57, 36, 0, 0, 3]	$\mathbf{1}_G$	1	8	[37, 57, 36, 0, 0, 3]	C_2	2
14	[37, 57, 36, 0, 0, 3]	C_3	3	4	[37, 57, 36, 0, 0, 3]	S_3	6
373	[37, 58, 34, 0, 2, 2]	$\mathbf{1}_G$	1	24	[37, 58, 34, 0, 2, 2]	C_2	2
75, 674	[37, 59, 31, 3, 1, 2]	$\mathbf{1}_G$	1	159	[37, 59, 31, 3, 1, 2]	C_2	2
901	[37, 59, 32, 0, 4, 1]	$\mathbf{1}_G$	1	17	[37, 59, 32, 0, 4, 1]	C_2	2
213, 659	[37, 60, 28, 6, 0, 2]	$\mathbf{1}_G$	1	281	[37, 60, 28, 6, 0, 2]	C_2	2
2	[37, 60, 28, 6, 0, 2]	$C_2 \times C_2$	4	226, 802	[37, 60, 29, 3, 3, 1]	$\mathbf{1}_G$	1
136	[37, 60, 29, 3, 3, 1]	C_2	2	1, 645, 639	[37, 61, 26, 6, 2, 1]	$\mathbf{1}_G$	1
407	[37, 61, 26, 6, 2, 1]	C_2	2	1, 331, 654	[37, 62, 23, 9, 1, 1]	$\mathbf{1}_G$	1
364	[37, 62, 23, 9, 1, 1]	$C_2 \times C_2$	4	137, 751	[37, 63, 20, 12, 0, 1]	$\mathbf{1}_G$	1
51	[37, 63, 20, 12, 0, 1]	C_2	2	24, 070	[38, 56, 34, 2, 1, 2]	$\mathbf{1}_G$	1
293	[38, 56, 34, 2, 1, 2]	C_2	2	184, 272	[38, 57, 31, 5, 0, 2]	$\mathbf{1}_G$	1
1	[38, 57, 31, 5, 0, 2]	C_{10}	10	603	[38, 57, 31, 5, 0, 2]	C_2	2
7	[38, 57, 31, 5, 0, 2]	$C_2 \times C_2$	4	2	[38, 57, 31, 5, 0, 2]	C_5	5
91, 653	[38, 57, 32, 2, 3, 1]	$\mathbf{1}_G$	1	376	[38, 57, 32, 2, 3, 1]	C_2	2
6	[38, 57, 32, 2, 3, 1]	$C_2 \times C_2$	4	1, 869, 994	[38, 58, 29, 5, 2, 1]	$\mathbf{1}_G$	1
1180	[38, 58, 29, 5, 2, 1]	C_2	2	3, 307, 896	[38, 59, 26, 8, 1, 1]	$\mathbf{1}_G$	1
2, 404	[38, 59, 26, 8, 1, 1]	C_2	2	15	[38, 59, 26, 8, 1, 1]	$C_2 \times C_2$	4
707, 690	[38, 60, 23, 11, 0, 1]	$\mathbf{1}_G$	1	1, 400	[38, 60, 23, 11, 0, 1]	C_2	2
3, 108	[39, 53, 37, 1, 1, 2]	$\mathbf{1}_G$	1	33	[39, 53, 37, 1, 1, 2]	C_2	2
80, 418	[39, 54, 34, 4, 0, 2]	$\mathbf{1}_G$	1	311	[39, 54, 34, 4, 0, 2]	C_2	2

No. of arcs	Arc type	G	$ G $	No. of arcs	Arc type	G	$ G $
4	[35, 66, 22, 8, 0, 2]	$C_2 \times C_2$	4	15, 190	[39, 54, 35, 1, 3, 1]	$\mathbf{1}_G$	1
30	[39, 54, 35, 1, 3, 1]	C_2	2	1, 083, 083	[39, 55, 32, 4, 2, 1]	$\mathbf{1}_G$	1
553	[39, 55, 32, 4, 2, 1]	C_2	2	4, 357, 859	[39, 56, 29, 7, 1, 1]	$\mathbf{1}_G$	1
698	[39, 56, 29, 7, 1, 1]	C_2	2	1, 893, 196	[39, 57, 26, 10, 0, 1]	$\mathbf{1}_G$	1
473	[39, 57, 26, 10, 0, 1]	C_2	2	141	[40, 50, 40, 0, 1, 2]	$\mathbf{1}_G$	1
29	[40, 50, 40, 0, 1, 2]	C_2	2	5	[40, 50, 40, 0, 1, 2]	$C_2 \times C_2$	4
2	[40, 50, 40, 0, 1, 2]	C_4	4	17, 241	[40, 51, 37, 3, 0, 2]	$\mathbf{1}_G$	1
228	[40, 51, 37, 3, 0, 2]	C_2	2	792	[40, 51, 38, 0, 3, 1]	$\mathbf{1}_G$	1
35	[40, 51, 38, 0, 3, 1]	C_2	2	309, 928	[40, 52, 35, 3, 2, 1]	$\mathbf{1}_G$	1
324	[40, 52, 35, 3, 2, 1]	C_2	2	9	[40, 52, 35, 3, 2, 1]	$C_2 \times C_2$	4
3, 041, 236	[40, 53, 32, 6, 1, 1]	$\mathbf{1}_G$	1	2, 319	[40, 53, 32, 6, 1, 1]	C_2	2
3	[40, 53, 32, 6, 1, 1]	$C_2 \times C_2$	4	2, 724, 024	[40, 54, 29, 9, 0, 1]	$\mathbf{1}_G$	1
2, 037	[40, 54, 29, 9, 0, 1]	C_2	2	15	[40, 54, 29, 9, 0, 1]	$C_2 \times C_2$	4
1, 634	[41, 48, 40, 2, 0, 2]	$\mathbf{1}_G$	1	83	[41, 48, 40, 2, 0, 2]	C_2	2
2	[41, 48, 40, 2, 0, 2]	$C_2 \times C_2$	4	41, 956	[41, 49, 38, 2, 2, 1]	$\mathbf{1}_G$	1
215	[41, 49, 38, 2, 2, 1]	C_2	2	1, 126, 688	[41, 50, 35, 5, 1, 1]	$\mathbf{1}_G$	1
446	[41, 50, 35, 5, 1, 1]	C_2	2	2, 138, 007	[41, 51, 32, 8, 0, 1]	$\mathbf{1}_G$	1
837	[41, 51, 32, 8, 0, 1]	C_2	2	49	[42, 45, 43, 1, 0, 2]	$\mathbf{1}_G$	1
24	[42, 45, 43, 1, 0, 2]	C_2	2	2, 383	[42, 46, 41, 1, 2, 1]	$\mathbf{1}_G$	1
19	[42, 46, 41, 1, 2, 1]	C_2	2	215, 487	[42, 47, 38, 4, 1, 1]	$\mathbf{1}_G$	1
659	[42, 47, 38, 4, 1, 1]	C_2	2	6	[42, 47, 38, 4, 1, 1]	$C_2 \times C_2$	4
918, 553	[42, 48, 35, 7, 0, 1]	$\mathbf{1}_G$	1	967	[42, 48, 35, 7, 0, 1]	C_2	2
2	[43, 42, 46, 0, 0, 2]	C_{10}	10	1	[43, 42, 46, 0, 0, 2]	C_2	2
1	[43, 42, 46, 0, 0, 2]	$C_2 \times C_2$	4	40	[43, 43, 44, 0, 2, 1]	$\mathbf{1}_G$	1
15	[43, 43, 44, 0, 2, 1]	$C_2 \times C_2$	4	20, 743	[43, 44, 41, 3, 1, 1]	$\mathbf{1}_G$	1
66	[43, 44, 41, 3, 1, 1]	C_2	2	214, 815	[43, 45, 38, 6, 0, 1]	$\mathbf{1}_G$	1
461	[43, 45, 38, 6, 0, 1]	C_2	2	835	[44, 41, 44, 2, 1, 1]	$\mathbf{1}_G$	1
46	[44, 41, 44, 2, 1, 1]	$\mathbf{1}_G$	1	26, 925	[44, 42, 41, 5, 0, 1]	$\mathbf{1}_G$	1
155	[44, 42, 41, 5, 0, 1]	C_2	2	6	[44, 42, 41, 5, 0, 1]	$C_2 \times C_2$	4
17	[45, 38, 47, 1, 1, 1]	$\mathbf{1}_G$	1	3	[45, 38, 47, 1, 1, 1]	C_2	2
1, 739	[45, 39, 44, 4, 0, 1]	$\mathbf{1}_G$	1	67	[45, 39, 44, 4, 0, 1]	C_2	2
63	[46, 36, 47, 3, 0, 1]	$\mathbf{1}_G$	1	10	[46, 36, 47, 3, 0, 1]	C_2	2
1	[47, 33, 50, 2, 0, 1]	$\mathbf{1}_G$	1	2	[47, 33, 50, 2, 0, 1]	C_2	2

4.4 The projectively distinct $(13, 5)$ –arcs

The distributed calculation of $(13, 5)$ -arcs in $\text{PG}(2, 11)$ took an input 30,221,738 arcs of length 12 calculated at the previous stage and represented in Table 4.2, split them into blocks, which may be processed independently, calculated all arcs of length 13 that can be produced by them, and then merged the results together and eliminated duplicates to determine their total number which is 415,776,269. The running time for $(13, 5)$ –arcs took about two months using 128 cores, and required an additional code for merging the result and eliminating duplicates, since the complete list of arcs was no longer fitting into the operative memory. The volume of storage required for this stage was 133 compressed files of total size 1.42 GB.

Theorem 4.4.1. *In $\text{PG}(2, 11)$, there are exactly 415,776,269 projectively distinct $(13, 5)$ –arcs.*

At this stage, we decided to stop experimental research using GAP since continuing to the next step and getting arcs of length 14 is beyond practical reachability.

Chapter 5

Combinatorial Classification Algorithms for Large Arcs in $\text{PG}(2, q)$

The classification of arcs is an instance of the classification problem of combinatorial objects. This is a difficult problem in general. Different algorithms have been developed. We describe two of them. The first algorithm is based on canonical forms. Since canonical form algorithms for graphs are readily available, for instance in the software package Nauty [29], we describe a way to reduce the problem of classifying arcs up to isomorphism to the problem of classifying a class of graphs up to isomorphism. The class of graphs that we need are the modified Levi graphs of the incidence geometry. This will be covered in Sections 5.1- 5.3. In Section 5.4, a different technique called Poset classification is described. This algorithm creates and classifies combinatorial objects at the same time, and it performs well on problems in finite geometry.

All results in this chapter are obtained using the open-source software package Orbiter [10]. Also, the program package Nauty is used through Orbiter, using the interface that was written by *Abdullah ALAzemi* from Kuwait University.

5.1 General definitions

Definition 5.1.1. Let α_{ij} and β_{ij} be a non-negative integers, a tactical decomposition of an incidence structure $\text{PG}(2, q) = (\mathcal{P}, \mathcal{L}, \mathcal{I})$, is any partition of the points in \mathcal{P} and the lines in \mathcal{L} ;

$$\mathcal{P} = \bigcup_{i=1}^m \mathcal{P}_i \quad \text{and} \quad \mathcal{L} = \bigcup_{j=1}^n \mathcal{L}_j.$$

such that:

1. each point of \mathcal{P}_i lies on exactly α_{ij} of \mathcal{L}_j ;

2. each line of \mathcal{L}_j contains exactly β_{ij} points of \mathcal{P}_i .

The decomposition is displayed in matrix form; the matrices $[\alpha_{ij}]$ and $[\beta_{ij}]$ are called the point-tactical decomposition and the line-tactical decomposition

Definition 5.1.2. A graph Γ is a pair (V, E) where V is a set of elements that are called vertices, and E is a set of pairs of V .

Definition 5.1.3. Two graphs $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ are called isomorphic if there exists a bijection $\varphi : V_1 \rightarrow V_2$ such that

$$\{v_1, v_2\} \in E_1 \iff \{\varphi(v_1), \varphi(v_2)\} \in E_2.$$

Definition 5.1.4. Let V be the set of vertices of a graph Γ . The adjacency matrix of Γ is the $n \times n$ matrix M with entries m_{ij} defined as follows:

$$m_{ij} = \begin{cases} 1 & \text{if there exists an edge between } v_i \text{ and } v_j \\ 0 & \text{otherwise.} \end{cases}$$

Definition 5.1.5. . A *bipartite* graph (V, E) is a graph whose vertices can be partitioned into two disjoint subsets A and B whose elements are pairwise non-adjacent. That is, every edge joins a vertex in A to a vertex in B .

Definition 5.1.6. . An incidence graph or a Levi graph Γ of the projective plane $\Pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ is the bipartite graph (V, E) where V is the set of points and lines of Π , with the property that if a point P lies on a line l then there exists an edge between P and l such that:

$$V = \mathcal{P} \cup \mathcal{L},$$

$$E = \{(p, l) \mid p \in \mathcal{P}, l \in \mathcal{L}, \text{ and } p \in l\}.$$

Definition 5.1.6 is adapted from [17] where you find more details about the Levi graph of such a configuration.

Definition 5.1.7. Let \mathcal{K} be a (k, n) -arc in $\text{PG}(2, q) = (\mathcal{P}, \mathcal{L})$. In the incidence matrix M of $\text{PG}(2, q)$, we have points and lines as is stated in Definition 2.2.12; there is 1 if a point p lies on the line l , otherwise it is 0. Next, extending M by one extra column that so-called "special line", l_k , and one extra row called "special point" p_k . This line l_k encodes the set \mathcal{K} ; namely l_k will have the arc points in \mathcal{K} . So we get the following extended incidence matrix M' .

$$\left[\begin{array}{c|c} & M' \\ \hline \text{The transpose of } M' & \end{array} \right]$$

Figure 5.1: The adjacency matrix of a Levi graph

$$M' = \left[\begin{array}{cccc|c} & & & & 1 \\ & & & & 1 \\ & & & & \vdots \\ & & & & 1 \\ \hline 0 & 0 & \dots & 0 & 1 \end{array} \right]$$

The entries of the extra row are all 0 except the last entry is 1 to show that we have the extra column that is the special line.

The Levi graph Γ of the new incidence configuration in Figure 5.1, associated with M' is the bipartite graph $\Gamma = (V, E_{\mathcal{K}})$ where

$$V = \{\mathcal{P} \cup \{p_k\} \cup \mathcal{L} \cup \{l_k\}\},$$

$$E_{\mathcal{K}} = \{(p, l) \mid p \in \mathcal{P}, l \in \mathcal{L}, \text{ and } p \in l\} \cup \{(p_k, l_k)\} \cup \{(p, l_k) \mid p \in \mathcal{K}\}.$$

Here the set of vertices V has $2q^2 + 2q + 4$ elements which is the union of points and lines; by points here we include the special point p_k . Also by lines here we include the special line l_k .

This bipartite graph is formed by a vertex for each point including the special one and a vertex for each line including the special line. The vertices of this graph are divided into two different classes. Therefore, there is no edge between vertices in the same class. The dimension of the adjacency matrix visualised in Figure 5.1 is $(2q^2 + 2q + 4) \times (2q^2 + 2q + 4)$.

Definition 5.1.8. Let \mathcal{G}_{2q^2+2q+4} be the set of graphs on $2q^2 + 2q + 4$ vertices. Then the canonical form \mathcal{C} is a function from \mathcal{G}_{2q^2+2q+4} to the permutations of $2q^2 + 2q + 4$ vertices:

$$\mathcal{C} : \mathcal{G}_{2q^2+2q+4} \mapsto \text{Sym}(2q^2 + 2q + 4)$$

such that

$$G \cong H \iff G^{C(G)} = H^{C(H)}, \forall G, H \in \mathcal{G}_{2q^2+2q+4}.$$

5.2 Isomorph classification of arcs in $\text{PG}(2, q)$ using canonical forms

The idea is that we have a set S of arcs in $\text{PG}(2, q)$ and we are interested in finding the classification of those arcs in S under the projective group of $\text{PG}(2, q)$. Following the same manner of Definition 5.1.7, we create for each arc in S a Levi graph out of an adjacency matrix as in Figure 5.1 that corresponds to each arc in S . Next, the Nauty program [29] computes the canonical labelling for these graphs in addition to the automorphism group of each arc. If two arcs have the same canonical labelling then they are projectively equivalent but if their canonical labellings are different then they are distinct up to projective equivalence.

5.3 Classification of objects in combinatorics

We consider Algorithm 4 to test if two sets are equivalent using the canonical forms defined in Definition 5.1.8. The method of canonical forms is a way of classifying sets; if two sets have identical canonical form then they are projectively equivalent, otherwise they are not.

In combinatorics, canonical forms are used to classify objects up to isomorphism. So, given sets A_1, A_2, \dots, A_m in $\text{PG}(2, q)$, we can classify these sets using Algorithm 4 which uses canonical forms. The dominant part in Algorithm 4 is in computing the canonical forms for all $A_i, i = 1, 2, \dots, m$.

On the other hand, using Algorithm 3 in Section 3.1 requires $\binom{m}{2}$ pairwise isomorphism tests. For this reason, it is better to use canonical forms for the classification. The canonical forms in this method are obtained using Nauty algorithm in [29].

Algorithm 4: Classify graphs A_1, A_2, \dots, A_m up to isomorphism.

Input: Graphs A_i where $i = 1, 2, \dots, m$

Output: A list L of the representatives of the distinct isomorphism classes among A_1, \dots, A_m .

$L := \emptyset, M := \emptyset$

for $i = 1$ to m **do**

 Compute $C(A_i)$ $\{C(A_i)$ is the canonical form of $A_i\}$

if $C(A_i) \notin M$ **then**

Add(L, A_i) **and** **Add**($M, C(A_i)$)

end if

end for

5.4 Poset classification

A large number of combinatorial problems involving classification can be reduced to classifying orbits of groups acting on partially ordered sets. The partially ordered set that we consider is the set of points in the plane which satisfy the condition that each line intersects this set in at most n points.

There are many different ways in which such a classification can be performed. First, there is the technique of **canonical augmentation**, developed by McKay [30]. It relies on the notion of canonical labelings. At present, the only implementation available is McKay's own Nauty [29]. The scarcity of canonical form algorithms and implementations leads us to look for different approaches. One alternative is an algorithm for poset-classification originally due to Schmalz [32]. For a modernized version, see [7]. The algorithm is available for many different posets, and an implementation in the software package Orbiter [10] can be used.

5.4.1 Some theory of the Poset classification algorithm

The basic piece in the poset classification algorithm is a lemma concerned with the orbits of a group G acting on an invariant relation \mathcal{R} . Let \mathcal{A} and \mathcal{B} be two disjoint finite sets. Suppose that \mathcal{R} is a relation between \mathcal{A} and \mathcal{B} . Thus $\mathcal{R} \subseteq \mathcal{A} \times \mathcal{B}$. The relation \mathcal{R} is a G -invariant; so

$$(a, b) \in \mathcal{R} \implies (a^g, b^g) \in \mathcal{R} \quad \forall g \in G.$$

Here we use exponential notation to indicate the group action. A pair $(a, b) \in \mathcal{R}$ is called a flag and an orbit of G on a flag in \mathcal{R} is called a flag-orbit. Every flag orbit is associated with exactly one orbit of G on \mathcal{A} and one orbit of G on \mathcal{B} .

Let π_1 and π_2 be the projection maps from $\mathcal{A} \times \mathcal{B}$ onto the first and second component. So, for $(a, b) \in \mathcal{A} \times \mathcal{B}$, we have $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$. For $a \in \mathcal{A}$, let

$$\text{Up}(a) = \{(a, b) \mid b \in \mathcal{B}, (a, b) \in \mathcal{R}\}$$

Also for $b \in \mathcal{B}$, let

$$\text{Down}(b) = \{(a, b) \mid a \in \mathcal{A}, (a, b) \in \mathcal{R}\}.$$

Let P_1, \dots, P_m be the orbit representatives for the orbits of G on \mathcal{A} ; namely, a transversal of the orbits of G on \mathcal{A} . Likewise, let Q_1, \dots, Q_n be the representatives for orbits of G on \mathcal{B} ; that is a

A				
$\bullet p_1$	$\bullet t_{11}$ T_{11}	$\bullet t_{12}$ T_{12}	\cdots	$\bullet t_{1r_1}$ T_{1r_1}
$\bullet p_2$	$\bullet t_{21}$ T_{21}	$\bullet t_{22}$ T_{22}	\cdots	$\bullet t_{2r_2}$ T_{2r_2}
\vdots	\vdots	\vdots		\vdots
$\bullet p_m$	$\bullet t_{m1}$ T_{m1}	$\bullet t_{m2}$ T_{m2}	\cdots	$\bullet t_{mr_m}$ T_{mr_m}

Table 5.1: The orbits $\mathcal{T}_{i,r}$ of $\text{Stab}_G(P_i)$ on $\text{Up}(P_i)$

transversal of the orbits of G on \mathcal{B} , so

$$\mathcal{A} = \bigcup_{i=1}^m \text{Orb}_G(P_i) \quad \text{and} \quad \mathcal{B} = \bigcup_{j=1}^n \text{Orb}_G(Q_j).$$

For $P_i \in \mathcal{A}$ and $i = 1, 2, \dots, m$, let the up-set of P_i be $\text{Up}(P_i) = \{(P_i, b) \mid b \in \mathcal{B}, (P_i, b) \in \mathcal{R}\}$, where $G_i = \text{Stab}_G(P_i)$ acts on $\text{Up}(P_i)$. For $r = 1, 2, \dots, R_i$, let $\mathcal{T}_{i,r}$ be the orbits of G_i on $\text{Up}(P_i)$ with orbit representatives $t_{i,r} = (P_i, b_{ir})$; so

$$\mathcal{T}_{ir} = \text{Orb}_{G_i}(t_{i,r}) \quad \text{and} \quad \text{Up}(P_i) = \bigcup_{r=1}^{R_i} \mathcal{T}_{ir}.$$

For $Q_j \in \mathcal{B}$ and $j = 1, 2, \dots, n$, let $H_j = \text{Stab}_G(Q_j)$ be the stabiliser of the Q_j in G . $\text{Down}(Q_j) = \{(a, Q_j) \mid a \in \mathcal{A}, (a, Q_j) \in \mathcal{R}\}$. Note that G_i acts on $\text{Up}(P_i)$ and H_j acts on $\text{Down}(Q_j)$.

For $l = 1, 2, \dots, L_j$, let \mathcal{S}_{jl} be the orbits of H_j on $\text{Down}(Q_j)$ and let $s_{j,l}$ be the orbit representatives of \mathcal{S}_{jl} ; so

$$\mathcal{S}_{jl} = \text{Orb}_{H_j}(s_{j,l}) \quad \text{and} \quad \text{Down}(Q_j) = \bigcup_{l=1}^{L_j} \mathcal{S}_{jl}.$$

The following Lemma from [8] relates the G -orbits on \mathcal{A} and the G -orbits on \mathcal{B} .

Lemma 5.4.1 ([9]). (1) *There is a canonical bijection between the set of orbits*

$$\{\mathcal{T}_{ir} \mid i = 1, \dots, m, \quad r = 1, \dots, R_i\}$$

and the set of orbits

$$\{\mathcal{S}_{jl} \mid j = 1, \dots, n, \quad l = 1, \dots, L_j\}.$$

$$(2) \quad \sum_{i=1}^m r_i = \sum_{j=1}^n l_j.$$

(3) *If \mathcal{T}_{ir} and \mathcal{S}_{jl} are corresponding orbits under the canonical bijection from 1, then*

$$|\text{Orb}_G(P_i)| \cdot |\mathcal{T}_{ir}| = |\text{Orb}_G(Q_j)| \cdot |\mathcal{S}_{jl}|.$$

B	$\bullet Q_1$	$\bullet Q_2$	\cdots	$\bullet Q_n$
	$\bullet s_{11}$ S_{11}	$\bullet s_{21}$ S_{21}	\cdots	$\bullet s_{n1}$ S_{n1}
	$\bullet s_{12}$ S_{12}	$\bullet s_{22}$ S_{22}	\cdots	$\bullet s_{n2}$ S_{n2}
	\vdots	\vdots		\vdots
	$\bullet s_{1L_1}$ S_{1L_1}	$\bullet s_{2L_2}$ S_{2L_2}	\cdots	$\bullet s_{nL_n}$ S_{nL_n}

Table 5.2: The orbits \mathcal{S}_{jl} of $\text{Stab}_G(Q_j)$ on $\text{Down}(Q_j)$

Chapter 6

Application of The Combinatorial Classification Algorithms for Large Arcs in $\text{PG}(2, 11)$

In this chapter, we applied the algorithms developed in Chapter 5 to the problem of classification of arcs of degree 3 and 4. The results for the classification problem of arcs in $\text{PG}(2, 11)$ are summarized in Sections 6.1- 6.4. In Section 6.1, we obtain arcs of degree three that are larger than any elliptic curve in this field. In Section 6.3, a lower bound for the number of 5-secants is derived, using Diophantine equations. In Section 6.4 a lower bound for the size of the smallest complete arc of degree 5 is derived. In Section 6.5, a technique due to Hill and Ball for constructing large arcs and multiple blocking sets is described. This technique is not complete classification, but often allows to create multiple isomorphism types of arcs. For instance, we find 134 isomorphism types of $(77, 8)$ -arcs.

6.1 Arcs of degree 3 in $\text{PG}(2, 11)$

Cook [13] classifies the arcs of degree 3 in $\text{PG}(2, 11)$. We are interested in (k, n) -arcs in $\text{PG}(2, 11)$ with $n > 3$, so that this result will be important for our work. We start by verifying this result using different techniques. Using Orbiter [10], a complete search have been done with the poset (partially ordered sets) classification algorithm. We confirm the numbers in the third column of Table 6.1. This table was first established in [13].

Cook finds exactly two isomorphism types of $(21, 3)$ -arcs in $\text{PG}(2, 11)$. These are the largest arcs of degree 3 in this plane. For more information on these arcs, see Table 6.2. In the table, Aut

Table 6.1: Number of the distinct $(k, 3)$ -arcs in $\text{PG}(2, 11)$

k	complete	incomplete	total
12	0	15,291,641	15291641
13	5	44,020,755	44,020,760
14	146	76,935,881	76,936,027
15	715,84,677	73086254	73,157,838
16	1,573,677	31,342,655	32,916,332
17	2,082,781	3801624	5,884,405
18	259,585	742,73	333,858
19	4,176	291	4,467
20	15	2	17
21	2	0	2

Table 6.2: Classification of $(21, 3)$ -arcs in $\text{PG}(2, 11)$

No. of Arcs	Aut	Line types	Point types
2	$C_7 \rtimes C_3$	[28, 21, 21, 63]	21 [1, 2, 9]

stands for the order of the automorphism group, line type is the vector

$$[\tau_0, \tau_1, \tau_2, \tau_3],$$

and point types are of the form

$$[\rho_1, \rho_2, \rho_3].$$

Interestingly, the largest $(k, 3)$ -arcs that we get from curves are elliptic curves whose number N_1 of points over \mathbf{F}_q reaches the Hasse-Weil upper bound:

$$N_1 \leq q + 1 + 2\sqrt{q}$$

Up to isomorphism, there are exactly two curves for which the number of points is 18, which is the value of the Hasse-Weil bound for $q = 11$ (cf. Table 6.3).

The curves were found using a classification algorithm for cubic curves in small projective planes developed by the authors. The software package Orbiter [10] was used. The internet table *Manypoints* [36] can be used to query the largest algebraic curves over small finite fields, and to find out references for the curves. For instance, elliptic curves with 18 points in $\text{PG}(2, 11)$ have been found by [34], and earlier work was done by Hasse [19] and Deuring [15]. Soomro in [34] lists the curve with equation $y^2 = x^3 + x + 3$, which is equivalent to the curve with automorphism group of order 6 in Table 6.3.

Table 6.3: Elliptic curves in PG(2, 11)

Equation	No. of pts	Aut	Line type
$5X_0^2X_1 + 10X_0^2X_2 + 6X_0X_1^2 +$ $10X_1^2X_2 + X_0X_2^2 + 2X_1X_2^2 + 10X_0X_1X_2$	18	3	[37, 66, 12, 18]
$7X_0^2X_1 + 8X_0^2X_2 + 4X_0X_1^2 +$ $8X_1^2X_2 + 3X_0X_2^2 + 4X_1X_2^2 + 10X_0X_1X_2$	18	6	[24, 48, 15, 46]

6.2 Arcs of degree 4 in PG(2, 11)

The largest arcs of degree 4 in PG(2, 11) have 32 points. Here is the classification of these arcs.

Theorem 6.2.1. *Up to isomorphism, there are exactly 210,692 complete (32, 4)-arcs in PG(2, 11).*

Information is given in Table 6.5 and 6.4.

Table 6.4: Point types of the (32, 4)-arcs

Notation	Point types
t_1	[1, 1, 0, 10]
t_2	[1, 0, 2, 9]
t_3	[0, 2, 1, 9]
t_4	[0, 1, 3, 8]
t_5	[0, 0, 5, 7]

Table 6.5: (32, 4)-arcs in PG(2, 11)

No. of Arcs	Aut	Line types	t_1	t_2	t_3	t_4	t_5
26945	D_{20}	[20, 2, 16, 30, 65]	2	0	10	10	10
34517	D_{20}	[10, 22, 16, 10, 75]	12	10	10	0	0
70078	C_{10}	[10, 22, 16, 10, 75]	12	10	10	0	0
79152	D_8	[12, 20, 10, 20, 71]	8	12	0	12	0

Cook [13] proves that to extend an $(s, 3)$ -arc to a $(33, 4)$ -arc in PG(2, 11), then $s \geq 12$. Cook [13] finds one arc in each line of Table 6.5. Our result is based on lifting all isomorphism types of $(s, 3)$ -arcs (complete and incomplete) from Table 6.1 for $12 \leq s \leq 21$. Parallel computing was used to perform this computation. The lifting of each arc is done by solving systems of Diophantine equations. The isomorph classification is done using Orbiter, which in turn relies on Nauty. The method of Levi graphs described in Section 5.2 is used.

Table 6.6: Known $(43, 5)$ -arcs in $\text{PG}(2, 11)$

	Aut	Lines type
Ball's arc	12	$[13, 0, 12, 3, 42, 63]$
New arc	10	$[15, 0, 3, 10, 45, 60]$

6.3 Arcs of degree 5 in $\text{PG}(2, 11)$

It is possible to increase the degree of an arc by adding points. The conditions for adding points can be expressed using Diophantine equations and inequalities. Suppose we want to extend the degree d of an arc by one. A d -secant can accept at most one new point. In general, a $d - i$ secant can accept $i + 1$ new points. For each line in the plane, one inequality is formed. Suppose we start from a (k, d) -arc and we wish to construct an $(s, d + 1)$ -arc for some $s > k$. The variables in the system are the points off the (k, d) -arc. One additional equation captures the fact that we want to add $s - k$ points. Consider an example, to construct a $(43, 5)$ -arc we try extending one of the $(32, 4)$ -arcs from Table 6.5. The first of these arcs can indeed be extended.

The new $(43, 5)$ -arc has a stabiliser group of order 10. Table 6.6 summarizes the known $(43, 5)$ -arcs in $\text{PG}(2, 11)$ as in [1].

The following theorem gives information about a putative $(45, 5)$ -arc.

Theorem 6.3.1. *In $\text{PG}(2, 11)$, the number of 5-secants of a $(45, 5)$ -arc satisfies the following bound:*

$$\tau_5 \geq 72.$$

Proof We consider the column-tactical decomposition scheme which is displayed below in the form of the incidence matrix of $\text{PG}(2, 11)$:

\downarrow	τ_5	τ_4	τ_3	τ_2	τ_1	τ_0
45	5	4	3	2	1	0
88	7	8	9	10	11	12

An arrow pointing downward in the top-left entry of the above incidence matrix is referring to a line-tactical decomposition.

For $q = 11$ and $n = 5$ the equations from Lemma 2.7.2 become the following:

$$\begin{aligned}
\sum_{j=0}^5 \binom{j}{2} \tau_j &= \binom{45}{2} = J_1 \\
\sum_{j=0}^5 \binom{12-j}{2} \tau_j &= \binom{88}{2} = J_2 \\
\sum_{j=0}^5 j(12-j) \tau_j &= 45 \cdot 88 = J_{1,2} \\
\sum_{j=0}^5 j \tau_j &= 45 \cdot 12 = F_1 \\
\sum_{j=0}^5 (12-j) \tau_j &= 88 \cdot 12 = F_2 \\
\sum_{j=0}^5 \tau_j &= 133 = C
\end{aligned}$$

Considering the above line-tactical decomposition scheme:

- equation J_1 counts the joining of pair of points in the first row of the scheme;
- equation J_2 counts the joining pair of points in the second row of the scheme;
- equation $J_{1,2}$ counts the joining of pair of points in first row with points in the second row;
- equation F_1 counts flags in row 1;
- equation F_2 counts flags in row 2.

In the table below RHS refers to the right hand side of the equations $J_1, J_2, J_{1,2}, F_1, F_2$, and C .

τ_5	τ_4	τ_3	τ_2	τ_1	τ_0	= RHS
10	6	3	1	0	0	990
21	28	36	45	55	66	3828
35	32	27	20	11	0	3928
5	4	3	2	1	0	540
7	8	9	10	11	12	1056
1	1	1	1	1	1	133

To show that $\tau_5 \geq 72$, we assume $\tau_5 \leq 71$ and show that the system has no solution.

Let $a_{i,j}$ be the entries in this matrix. Considering the second row, we deduce that

$$\tau_3 \leq \lfloor \frac{3828}{36} \rfloor = 106, \quad \tau_2 \leq \lfloor \frac{3828}{45} \rfloor = 85,$$

$$\tau_1 \leq \lfloor \frac{3828}{55} \rfloor = 69, \quad \text{and} \quad \tau_0 \leq \lfloor \frac{3828}{66} \rfloor = 58.$$

Note that $\lfloor x \rfloor$ refers to the floor function of x which is a function that maps a real number x to the greatest integer that is less than or equal to x . Also $\lceil x \rceil$ is the ceiling function which is the function that takes a real number x and maps it to the least number greater than or equal to x . Next, elementary row operations lead to

τ_5	τ_4	τ_3	τ_2	τ_1	τ_0	= RHS
10	6	3	1	0	0	990
0	1	6	15	28	45	765
0	10	15	15	10	0	450
5	4	3	2	1	0	540
0	2	4	6	8	10	250
1	1	1	1	1	1	133

Considering the second row, we deduce that $\frac{765}{45} = \tau_0 \leq 17$. This leaves 18 cases to consider for τ_0 . We perform a case-by-case analysis. Each case is similar, so we only look at one of the cases: $\tau_0 = 0$ (the hardest case). The general idea is to make lower and upper bounds for τ_j say

$$l_j \leq \tau_j \leq u_j.$$

Let $a_{i,j}$ be the (i,j) entry in the reduced coefficient matrix. If at some point

$$\sum_{j=0}^5 a_{i,j} u_j < \text{RHS}_i$$

for some equation i , then we know the system has no solution (the stopping rule). It remains to tighten the bounds l_j and u_j . The following two observations are helpful:

1. for all (i,j) we have

$$u_j \leq \left\lceil \frac{\text{RHS}_i - \sum_{\substack{h=0 \\ h \neq j}}^5 a_{i,h} l_h}{a_{i,j}} \right\rceil$$

2. for all (i,j) we have

$$l_j \geq \left\lfloor \frac{\text{RHS}_i - \sum_{\substack{h=0 \\ h \neq j}}^5 a_{i,h} u_h}{a_{i,j}} \right\rfloor$$

We consider all pairs (i,j) and tighten the bounds using the two observations. If an improvement is made, all pairs (i,j) are tested again. This is repeated until either there are no more improvements,

Table 6.7: Sharpening of bounds in the proof of Theorem 6.3.1

	τ_5	τ_4	τ_3	τ_2	τ_1	τ_0
Eqn. no.	$l_5 - u_5$	$l_4 - u_4$	$l_3 - u_3$	$l_2 - u_2$	$l_1 - u_1$	$l_0 - u_0$
	0 – 71	0 – 123	0 – 106	0 – 85	0 – 69	0
1	0 – 71	0 – 123	0 – 106	0 – 51	0 – 27	0
2	0 – 71	0 – 45	0 – 30	0 – 30	0 – 27	0
3	37 – 71	2 – 45	0 – 30	0 – 30	0 – 27	0
0	60 – 71	27 – 45	0 – 30	0 – 30	0 – 27	0
1	60 – 71	27 – 45	0 – 30	0 – 30	4 – 26	0
2	60 – 71	27 – 41	0 – 9	0 – 9	4 – 18	0
3	63 – 71	31 – 41	0 – 9	0 – 9	4 – 18	0
4	63 – 71	31 – 41	0 – 9	0 – 9	10 – 18	0
0	71 – 71	41 – 41	9 – 9	7 – 9	10 – 18	0

or for one equation i the stopping rule is reached. For $\tau_0 = 0$, this leads to the bounds shown in Table 6.7.

Recall:

	τ_5	τ_4	τ_3	τ_2	τ_1	τ_0	= RHS
$a_{1,j}$	0	1	6	15	28	45	765

and for $j = 0$

τ_5	τ_4	τ_3	τ_2	τ_1	τ_0
71 – 71	41 – 41	9 – 9	7 – 9	10 – 18	0

In Table 6.7, there are other equations but we ask the program to print out just the improved row values. At this point, the stopping rule is reached in equation $i = 1$:

$$\sum_{j=0}^5 a_{i,j} u_j = 0 \cdot 71 + 1 \cdot 41 + 6 \cdot 9 + 15 \cdot 9 + 28 \cdot 18 + 45 \cdot 0 = 734 < 765 = \text{RHS}_1$$

This means that the case $\tau_5 \leq 71$ and $\tau_0 = 0$ is ruled out. The other cases of τ_0 are dealt with in a similar fashion. This shows that $\tau_5 \geq 72$. \square

So far, no $(44, 5)$ -arc or $(45, 5)$ -arc is known but they have not been ruled out either. Using the lifting algorithm, we extend the four isomorphism types of the complete $(32, 4)$ -arcs in $\text{PG}(2, 11)$ to get $(44, 5)$ -arcs or $(45, 5)$ -arcs but it gives neither.

Conjecture 6.3.2. *Extending the largest complete arcs of degree 4 in $\text{PG}(2, 11)$, gives neither $(44, 5)$ -arcs nor $(45, 5)$ -arcs.*

6.4 The smallest complete arcs of degree 5 in $\text{PG}(2, 11)$

As mentioned in earlier chapters that arcs of degree 5 in $\text{PG}(2, 11)$ are subsets of $\text{PG}(2, 11)$ where the greatest number of collinear points is 5. The complete arcs of degree 5 in $\text{PG}(2, q)$ start to show up when $k = k'$ where $k' \geq \sqrt{(n-1)(q+1)}$ due to [23]. So, for $q = 11$; $k \geq 16$.

Then in [2], they prove that the smallest complete arc exists in $\text{PG}(2, q)$ when $k = k'$, where

$$k' \geq \frac{(q+1-n^2) + \sqrt{(q+1-n^2)^2 + 4(n^2-n)(q+1-n)(q^2+q+1)}}{2(q+1-n)}.$$

Which implies that the smallest complete arc in $\text{PG}(2, 11)$ exists when $k \geq 19$.

However, in the following theorem, we prove that there is no complete arc of degree 5 in $\text{PG}(2, 11)$ when $k = 19, 20$, and 21.

Theorem 6.4.1. *Let $(k, 5)$ -arc be the smallest complete arc of degree 5 in $\text{PG}(2, 11)$, then k must be at least 22.*

Proof We assume that $k = 19$, and consider the column-tactical decomposition scheme of the incidence matrix of $\text{PG}(2, 11)$ in Table 6.8. This gives 114 points outside the arc. Each point off the arc would have to lie on at least one 5-secant, otherwise it could be added to the arc, leading to a larger arc of degree 5. So we would need at least $\frac{114}{5} = 22.8$ rounded up many 5-secants. So $\tau_5 \geq 17$.

The standard equations from Lemma 2.7.2 gives the below equations $J_1, J_2, J_{1,2}, F_1, F_2$, and C :

- equation J_1 counts the joining of pair of points in row 1;
- equation J_2 counts the joining of pair of points in the second row of the scheme;
- equation $J_{1,2}$ counts the joining of pair of points in the first and the second row;
- equation F_1 counts flags in row 1;
- equation F_2 counts flags in row 2.

Table 6.8: The column-tactical decomposition scheme in $\text{PG}(2, 11)$

\downarrow	τ_5	τ_4	τ_3	τ_2	τ_1	τ_0
19	5	4	3	2	1	0
114	7	8	9	10	11	12

$$\begin{aligned}
\sum_{j=0}^5 \binom{j}{2} \tau_j &= \binom{19}{2} \quad J_1 \\
\sum_{j=0}^5 \binom{12-j}{2} \tau_j &= \binom{114}{2} \quad J_2 \\
\sum_{j=0}^5 j(12-j) \tau_j &= 19 \cdot 114 \quad J_{1,2} \\
\sum_{j=0}^5 j \tau_j &= 19 \cdot 12 \quad F_1 \\
\sum_{j=0}^5 (12-j) \tau_j &= 114 \cdot 12 \quad F_2 \\
\sum_{j=0}^5 \tau_j &= 133 \quad C
\end{aligned}$$

So,

τ_5	τ_4	τ_3	τ_2	τ_1	τ_0	= RHS
10	6	3	1	0	0	171
21	28	36	45	55	66	6441
35	32	27	20	11	0	2166
5	4	3	2	1	0	228
7	8	9	10	11	12	1368
1	1	1	1	1	1	133

By solving the above system we get $\tau_5 \leq 10$, a contradiction. Proceeding in the same manner we get a contradiction for the cases where $k = 20, 21$. This means that a complete $(k, 5)$ -arc in $\text{PG}(2, 11)$ has at least 22 points. \square

6.5 Large arcs and blocking sets

This construction method was first used by Hill [20] and subsequently by Simeon Ball [3]. Up to projective equivalence, there are 2 types of $(5, 2)$ -arcs in $\text{PG}(2, 11)$. We will consider a special type of those two arcs A to construct a $(77, 8)$ -arc in $\text{PG}(2, 11)$. We used the fact that constructing a maximum $(k, 8)$ -arc in $\text{PG}(2, 11)$ is equivalent to finding a minimum 4-fold blocking set by considering complements.

By duality, the points of the arc of degree 2 in $\text{PG}(2, 11)$ become lines in the dual plane. Let the set S be the dual of the arc A then S has 50 points such that

$$|S| = 5 * 12 - \binom{5}{2} = 50.$$

With respect to the arc A , the points of $\text{PG}(2, 11) \setminus A$ are divided into sets C_0, C_1 and C_2 where C_i is the set of points off the arc A that lie on i bisecants of A . Also the lines of $\text{PG}(2, 11)$ are split into a set B of 10 bisecants, 40 tangents in a set T , and 83 external lines in a set E . As shown in Table 6.9.

Consider the points outside the arc that have 2 bisecants through them, C_2 points, there are 15 points of them. These C_2 points form a $(15, 4)$ -arc with one 4-secant and eleven 3-secants as shown in the decomposition of the incidence matrix of $\text{PG}(2, 11)$ in Table 6.9.

The points in the dual plane that are covered or blocked twice, namely points off A that have 2 bisecant lines passing through them, correspond to bisecants in the original setting.

We assume $K = B \cup T \cup D$ where $D \subset E$ and K is the 4-fold blocking set. And in the dual plane, $B \cup T$ blocks

- the A -lines 12 times;
- the C_1 -lines 4 times;
- the C_0 -lines 5 times.

However the C_2 -lines cover only 3 points of $B \cup T$. In order to make K a 4-fold blocking set, we need to choose a set $D \subset E$ which blocks each C_2 point at least once. Since we are interested in large arcs we want the size of the blocking set K is as small as possible and hence its complement is a large degree 8 arc. Using the program, the smallest size of the set D we get is 6 which gives the $(56, 4)$ -blocking set K in $\text{PG}(2, 11)$. The complement of which is $(77, 8)$ -arcs, see Theorem 6.5.1.

Theorem 6.5.1. *Up to isomorphism, there are 134 arcs of degree 8 and size 77 in $\text{PG}(2, 11)$; 126 have identity group and 8 of them have a group of order 2. Their types $[\tau_0, \tau_1, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6, \tau_7, \tau_8]$ and groups are shown in Table 6.10.*

Table 6.9: The decomposition of the incidence matrix w.r.t. $(5, 2)$ -arc

<i>Points</i> \ <i>Lines</i>	$ B = 10$	$ T = 40$	$ E = 83$
$ A = 5$	$4 \setminus 2$	$8 \setminus 1$	$0 \setminus 0$
$ C_2 = 15$	$2 \setminus 3$	$1 \setminus$	$\geq 1 \setminus ?$
$ C_1 = 70$	$1 \setminus 7$	$3 \setminus$	
$ C_0 = 43$	$0 \setminus 0$	$5 \setminus$	

Table 6.10: The projectively distinct $(77, 8)$ -arcs in $\text{PG}(2, 11)$

No. of arcs	Arcs type	G	$ G $
1	$[5, 0, 1, 0, 0, 2, 21, 46, 58]$	$\mathbf{1}_G$	1
2	$[5, 0, 0, 1, 1, 3, 17, 48, 58]$	$\mathbf{1}_G$	1
1	$[5, 0, 0, 1, 1, 0, 26, 39, 61]$	$\mathbf{1}_G$	1
1	$[5, 0, 0, 1, 0, 3, 23, 40, 61]$	$\mathbf{1}_G$	1
3	$[5, 0, 0, 1, 0, 4, 20, 43, 60]$	$\mathbf{1}_G$	1
3	$[5, 0, 0, 1, 0, 5, 17, 46, 59]$	$\mathbf{1}_G$	1
1	$[5, 0, 0, 1, 0, 6, 14, 49, 58]$	$\mathbf{1}_G$	1
1	$[5, 0, 0, 0, 1, 2, 30, 30, 65]$	$\mathbf{1}_G$	1
1	$[5, 0, 0, 0, 1, 3, 27, 33, 64]$	$\mathbf{1}_G$	1
8	$[5, 0, 0, 0, 1, 4, 24, 36, 63]$	$\mathbf{1}_G$	1
12	$[5, 0, 0, 0, 1, 5, 21, 39, 62]$	$\mathbf{1}_G$	1
18	$[5, 0, 0, 0, 1, 6, 18, 42, 61]$	$\mathbf{1}_G$	1
1	$[5, 0, 0, 0, 1, 6, 18, 42, 61]$	C_2	2
6	$[5, 0, 0, 0, 1, 7, 15, 45, 60]$	$\mathbf{1}_G$	1
1	$[5, 0, 0, 0, 1, 7, 15, 45, 60]$	C_2	2
1	$[5, 0, 0, 0, 1, 9, 9, 51, 58]$	$\mathbf{1}_G$	1
3	$[5, 0, 0, 0, 2, 2, 24, 38, 62]$	$\mathbf{1}_G$	1
10	$[5, 0, 0, 0, 2, 3, 21, 41, 61]$	$\mathbf{1}_G$	1
1	$[5, 0, 0, 0, 2, 3, 21, 41, 61]$	C_2	2
11	$[5, 0, 0, 0, 2, 4, 18, 44, 60]$	$\mathbf{1}_G$	1
11	$[5, 0, 0, 0, 2, 5, 15, 47, 59]$	$\mathbf{1}_G$	1
1	$[5, 0, 0, 0, 2, 6, 12, 50, 58]$	$\mathbf{1}_G$	1
3	$[5, 0, 0, 0, 3, 2, 18, 46, 59]$	$\mathbf{1}_G$	1
1	$[5, 0, 0, 0, 3, 3, 15, 49, 58]$	$\mathbf{1}_G$	1
1	$[5, 0, 0, 0, 3, 4, 12, 52, 57]$	C_2	2
2	$[5, 0, 0, 0, 0, 5, 27, 31, 65]$	$\mathbf{1}_G$	1
10	$[5, 0, 0, 0, 0, 6, 24, 34, 64]$	$\mathbf{1}_G$	1
7	$[5, 0, 0, 0, 0, 7, 21, 37, 63]$	$\mathbf{1}_G$	1
2	$[5, 0, 0, 0, 0, 7, 21, 37, 63]$	C_2	2
5	$[5, 0, 0, 0, 0, 8, 18, 40, 62]$	$\mathbf{1}_G$	1
3	$[5, 0, 0, 0, 0, 9, 15, 43, 61]$	$\mathbf{1}_G$	1
1	$[5, 0, 0, 0, 0, 9, 15, 43, 61]$	C_2	2
1	$[5, 0, 0, 0, 0, 10, 12, 46, 60]$	C_2	2
134	Total No. of Arcs		

This technique of constructing large arcs in Section 6.5 has been programmed and added to Orbiter library as a tool to construct large arcs and blocking sets. All the related commands are explained in Appendix B.2.

Chapter 7

Conclusion and Future Work

7.1 Conclusions

The principle aim of this thesis is the classification of $(k, 5)$ -arcs up to projective equivalence in $\text{PG}(2, 11)$ and to find the largest value of k for which a $(k, 5)$ -arc exists which we denote by $m_5(2, 11)$. Ball [3] proved that $43 \leq m_5(2, 11) \leq 45$. The problem of classification is best addressed in the language of groups acting on sets. So, I designed with the help of my advisor a classification algorithm for arcs that are generated by the group action. By implementing this algorithm in GAP [35], we succeed in proving the new exact numbers of the projectively distinct arcs of length $5 \leq k \leq 13$. These new results are stated in Theorems 3.3.1, 3.4.1, 3.5.1, 3.6.1, 3.7.1 and 3.8.1 in Chapter 3 and in Theorems 4.2.1, 4.3.1 and 4.4.1 of Chapter 4. We ran the GAP code in parallel to find these results, as the number of the arcs is large, but stopped using it after $k = 13$. The exponential growth of the data was no longer fitting into the main memory. The next stage where $k = 14$ would be beyond practical reachability.

We conclude that testing projective equivalence on arcs is time consuming and we need more efficient algorithms to deal with it. Also we decided to look at the structures of arcs of degree 3 and 4 in $\text{PG}(2, 11)$ which helped us later to get a new example of the complete $(43, 5)$ -arc shown in Table 6.6.

Graphs are normally classified using canonical forms. An implementation of the canonical forms algorithm is available in the software package Nauty [29]. In Section 5.2, we describe a new way to reduce the problem of classifying arcs up to isomorphism into the problem of classifying a class of graphs up to isomorphism. We used the program package Nauty through Orbiter, using the interface that was written for this project by *Abdullah AlAzemi* from Kuwait University.

In Chapter 6, we were the first in applying a combinatorial algorithm called the Poset classi-

fication algorithm to the problem of classification of the $(k, 3)$ -arcs in $\text{PG}(2, 11)$. This algorithm is implemented in the library of the software package Orbiter therefore we used it to perform our classification. We obtain two isomorphism types of $(21, 3)$ -arcs that are larger than any elliptic curves in this field. We also developed a new algorithm to classify cubic curves over small finite fields and made it available in the Orbiter library.

Cook [13] classifies $(32, 4)$ -arcs in $\text{PG}(2, 11)$ and only found one example of each isomorphism type but we proved using different technique that there are exactly 210,692 complete $(32, 4)$ -arcs, see Theorem 6.2.1.

By solving a system of Diophantine equations we proved that $t_5(2, 11) \geq 22$, see Theorem 6.4.1. This is the minimum value of k for which a complete $(k, 5)$ -arc exists. This result is different from the previous known results [2] [23] where they proved that $t_5(2, 11) \geq 19$ and $t_5(2, 11) \geq 16$ respectively. We also contributed to the problem of deciding the existence of a $(45, 5)$ -arc by proving a new lower bound for the number of 5-secants of the $(45, 5)$ -arcs in $\text{PG}(2, 11)$, see Theorem 6.3.1. We also conjecture the non existence of $(44, 5)$ -arcs or $(45, 5)$ -arcs formed by extending the four isomorphism types of the complete $(32, 4)$ -arcs $\text{PG}(2, 11)$, see Conjecture 6.3.2. We constructed 134 new isomorphism types of $(77, 8)$ -arc using the configuration of an arc of degree 2 in $\text{PG}(2, 11)$ and considering the complement relation with the blocking sets. This approach unlike other construction methods gives multiple isomorphism types of arcs.

The main application of classifying (k, n) -arcs in Coding Theory is the study of linear codes, as (k, n) -arcs and a linear $[k, 3, k - n]$ -codes are equivalent objects.

7.2 Recommendation for Future Research

The technique of constructing large arcs of degree 7 in $\text{PG}(2, 11)$ that we developed in Section 6.5 of this thesis indicates a recommendation to use the same technique to construct large arcs of degree 5 in the same projective plane which we think is worth further investigation. We recommend using this approach to construct large arcs as it gives multiple isomorphism types of arcs unlike other construction methods which normally give one arc.

In this section, we describe a construction method to get a complete arc of degree 5 by considering its complement link with the 7-fold blocking set. To construct a large arc of degree 5 we will use the configuration of $(9, 2)$ -arc A in $\text{PG}(2, 11)$. Let B be the set of bisecants of A , T be the set of tangents, E be the set of external lines and C_i be the set of points not in A that they lie on exactly i -bisecants. We assume that $K = B \cup T \cup D$ where $D \subset E$ as shown in the decomposition of the incidence matrix of $\text{PG}(2, 11)$ in Table 7.1.

In the dual plane, $B \cup T$ blocks the A -lines 12 times, the C_0 -lines 9 times, the C_1 -lines 8 times and the C_2 -lines 7 times. However, the lines of C_3 contain only 6 points of $B \cup T$, and the lines of

Table 7.1: The decomposition of the incidence matrix w.r.t. $(9, 2)$ -arcs

$P_i \backslash L_i$	B	T	E
A	$8 \setminus 2$	$4 \setminus 1$	$0 \setminus 0$
C_0	$0 \setminus 0$	$9 \setminus$	$3 \setminus$
C_1	$1 \setminus$	$7 \setminus$	$4 \setminus$
C_2	$2 \setminus$	$5 \setminus$	$5 \setminus$
C_3	$3 \setminus$	$3 \setminus$	$6 \setminus$
C_4	$4 \setminus$	$1 \setminus$	$7 \setminus$

C_4 contain only 5 points of $B \cup T$. In order to make K a 7-fold blocking set, we need to choose a set $D \subset E$, which blocks each C_3 -line at least once and each C_4 -line at least twice. Since we are interested in large arcs S , we want the blocking set $K = \mathcal{P} \setminus S$ is as small as possible. We are interested in finding the smallest set $D \subset E$ satisfying the conditions:

- (1) each C_3 -line is blocked at least once;
- (2) each C_4 -line is blocked at least twice.

Up to isomorphism, there are five isomorphism types of $(9, 2)$ -arcs in $\text{PG}(2, 11)$. These arcs points in Table 7.2 are in Orbiter format, see Appendix B.1. In this table, $|E|$ refers to the number of external lines with respect to each $(9, 2)$ -arc in $\text{PG}(2, 11)$, $|B|$ refers to the number of bisecants and $|C_2\text{-pts}|$ refers to the number of C_2 -points.

Table 7.2: The projectively distinct $(9, 2)$ -arcs in $\text{PG}(2, 11)$

Arc	$ G $	$ E $	$ B $	$ C_2\text{-pts} $
$\{0, 1, 2, 3, 37, 47, 61, 86, 115\}$	6	61	36	123
$\{0, 1, 2, 3, 37, 47, 65, 83, 99\}$	6	61	36	121
$\{0, 1, 2, 3, 37, 47, 73, 105, 129\}$	2	61	36	120
$\{0, 1, 2, 3, 37, 47, 77, 85, 127\}$	3	61	36	121
$\{0, 1, 2, 3, 37, 54, 74, 80, 93\}$	6	61	36	121

Appendices

Appendix A

GAP codes and labelling of points in $\text{PG}(2, 11)$

A.1 GAP package FinIng labelling [6]

$P_1 = (1, 0, 0)$	$P_{20} = (1, 5, 1)$	$P_{39} = (0, 1, 3)$	$P_{58} = (1, 7, 4)$
$P_2 = (0, 1, 0)$	$P_{21} = (1, 6, 1)$	$P_{40} = (1, 1, 3)$	$P_{59} = (1, 8, 4)$
$P_3 = (1, 1, 0)$	$P_{22} = (1, 7, 1)$	$P_{41} = (1, 2, 3)$	$P_{60} = (1, 9, 4)$
$P_4 = (1, 2, 0)$	$P_{23} = (1, 8, 1)$	$P_{42} = (1, 3, 3)$	$P_{61} = (1, 10, 4)$
$P_5 = (1, 3, 0)$	$P_{24} = (1, 9, 1)$	$P_{43} = (1, 4, 3)$	$P_{62} = (1, 0, 5)$
$P_6 = (1, 4, 0)$	$P_{25} = (1, 10, 1)$	$P_{44} = (1, 5, 3)$	$P_{63} = (0, 1, 5)$
$P_7 = (1, 5, 0)$	$P_{26} = (1, 0, 2)$	$P_{45} = (1, 6, 3)$	$P_{64} = (1, 1, 5)$
$P_8 = (1, 6, 0)$	$P_{27} = (0, 1, 2)$	$P_{46} = (1, 7, 3)$	$P_{65} = (1, 2, 5)$
$P_9 = (1, 7, 0)$	$P_{28} = (1, 1, 2)$	$P_{47} = (1, 8, 3)$	$P_{66} = (1, 3, 5)$
$P_{10} = (1, 8, 0)$	$P_{29} = (1, 2, 2)$	$P_{48} = (1, 9, 3)$	$P_{67} = (1, 4, 5)$
$P_{11} = (1, 9, 0)$	$P_{30} = (1, 3, 2)$	$P_{49} = (1, 10, 3)$	$P_{68} = (1, 5, 5)$
$P_{12} = (1, 10, 0)$	$P_{31} = (1, 4, 2)$	$P_{50} = (1, 0, 4)$	$P_{69} = (1, 6, 5)$
$P_{13} = (0, 0, 1)$	$P_{32} = (1, 5, 2)$	$P_{51} = (0, 1, 4)$	$P_{70} = (1, 7, 5)$
$P_{14} = (1, 0, 1)$	$P_{33} = (1, 6, 2)$	$P_{52} = (1, 1, 4)$	$P_{71} = (1, 8, 5)$
$P_{15} = (0, 1, 1)$	$P_{34} = (1, 7, 2)$	$P_{53} = (1, 2, 4)$	$P_{72} = (1, 9, 5)$
$P_{16} = (1, 1, 1)$	$P_{35} = (1, 8, 2)$	$P_{54} = (1, 3, 4)$	$P_{73} = (1, 10, 5)$
$P_{17} = (1, 2, 1)$	$P_{36} = (1, 9, 2)$	$P_{55} = (1, 4, 4)$	$P_{74} = (1, 0, 6)$
$P_{18} = (1, 3, 1)$	$P_{37} = (1, 10, 2)$	$P_{56} = (1, 5, 4)$	$P_{75} = (0, 1, 6)$
$P_{19} = (1, 4, 1)$	$P_{38} = (1, 0, 3)$	$P_{57} = (1, 6, 4)$	$P_{76} = (1, 1, 6)$

$P_{77} = (1, 2, 6)$	$P_{92} = (1, 5, 7)$	$P_{107} = (1, 8, 8)$	$P_{122} = (1, 0, 10)$
$P_{78} = (1, 3, 6)$	$P_{93} = (1, 6, 7)$	$P_{108} = (1, 9, 8)$	$P_{123} = (0, 1, 10)$
$P_{79} = (1, 4, 6)$	$P_{94} = (1, 7, 7)$	$P_{109} = (1, 10, 8)$	$P_{124} = (1, 1, 10)$
$P_{80} = (1, 5, 6)$	$P_{95} = (1, 8, 7)$	$P_{110} = (1, 0, 9)$	$P_{125} = (1, 2, 10)$
$P_{81} = (1, 6, 6)$	$P_{96} = (1, 9, 7)$	$P_{111} = (1, 1, 9)$	$P_{126} = (1, 3, 10)$
$P_{82} = (1, 7, 6)$	$P_{97} = (1, 10, 7)$	$P_{112} = (1, 1, 9)$	$P_{127} = (1, 4, 10)$
$P_{83} = (1, 8, 6)$	$P_{98} = (1, 0, 8)$	$P_{113} = (1, 2, 9)$	$P_{128} = (1, 5, 10)$
$P_{84} = (1, 9, 6)$	$P_{99} = (1, 1, 8)$	$P_{114} = (1, 3, 9)$	$P_{129} = (1, 6, 10)$
$P_{85} = (1, 10, 6)$	$P_{100} = (1, 1, 8)$	$P_{115} = (1, 4, 9)$	$P_{130} = (1, 7, 10)$
$P_{86} = (1, 0, 7)$	$P_{101} = (1, 2, 8)$	$P_{116} = (1, 5, 9)$	$P_{131} = (1, 8, 10)$
$P_{87} = (0, 1, 7)$	$P_{102} = (1, 3, 8)$	$P_{117} = (1, 6, 9)$	$P_{132} = (1, 9, 10)$
$P_{88} = (1, 1, 7)$	$P_{103} = (1, 4, 8)$	$P_{118} = (1, 7, 9)$	$P_{133} = (1, 10, 10)$
$P_{89} = (1, 2, 7)$	$P_{104} = (1, 5, 8)$	$P_{119} = (1, 8, 9)$	
$P_{90} = (1, 3, 7)$	$P_{105} = (1, 6, 8)$	$P_{120} = (1, 9, 9)$	
$P_{91} = (1, 4, 7)$	$P_{106} = (1, 7, 8)$	$P_{121} = (1, 10, 9)$	

A.2 GAP system labelling [35]

$P_1 = (1, 0, 0)$	$P_{18} = (1, 4, 5)$	$P_{35} = (1, 2, 4)$	$P_{52} = (1, 1, 1)$
$P_2 = (1, 0, 10)$	$P_{19} = (1, 6, 6)$	$P_{36} = (1, 6, 2)$	$P_{53} = (1, 8, 7)$
$P_3 = (1, 0, 5)$	$P_{20} = (1, 4, 8)$	$P_{37} = (1, 7, 3)$	$P_{54} = (1, 1, 4)$
$P_4 = (1, 10, 10)$	$P_{21} = (1, 3, 6)$	$P_{38} = (1, 7, 8)$	$P_{55} = (1, 10, 7)$
$P_5 = (1, 0, 8)$	$P_{22} = (1, 2, 1)$	$P_{39} = (1, 1, 6)$	$P_{56} = (1, 6, 1)$
$P_6 = (1, 5, 10)$	$P_{23} = (1, 4, 4)$	$P_{40} = (1, 4, 7)$	$P_{57} = (1, 9, 8)$
$P_7 = (1, 5, 5)$	$P_{24} = (1, 7, 6)$	$P_{41} = (1, 3, 2)$	$P_{58} = (1, 2, 7)$
$P_8 = (0, 1, 1)$	$P_{25} = (0, 1, 6)$	$P_{42} = (1, 9, 3)$	$P_{59} = (1, 5, 2)$
$P_9 = (1, 0, 4)$	$P_{26} = (1, 6, 0)$	$P_{43} = (1, 9, 4)$	$P_{60} = (1, 5, 7)$
$P_{10} = (1, 8, 10)$	$P_{27} = (1, 0, 1)$	$P_{44} = (1, 3, 0)$	$P_{61} = (1, 3, 1)$
$P_{11} = (1, 8, 5)$	$P_{28} = (1, 2, 10)$	$P_{45} = (1, 0, 3)$	$P_{62} = (1, 5, 3)$
$P_{12} = (1, 9, 9)$	$P_{29} = (1, 2, 5)$	$P_{46} = (1, 0, 6)$	$P_{63} = (1, 10, 4)$
$P_{13} = (1, 8, 8)$	$P_{30} = (1, 2, 2)$	$P_{47} = (1, 1, 10)$	$P_{64} = (1, 6, 3)$
$P_{14} = (1, 10, 9)$	$P_{31} = (1, 2, 8)$	$P_{48} = (1, 1, 5)$	$P_{65} = (1, 3, 5)$
$P_{15} = (1, 1, 0)$	$P_{32} = (1, 1, 2)$	$P_{49} = (1, 7, 7)$	$P_{66} = (1, 2, 9)$
$P_{16} = (1, 0, 2)$	$P_{33} = (1, 3, 3)$	$P_{50} = (1, 1, 8)$	$P_{67} = (1, 8, 2)$
$P_{17} = (1, 4, 10)$	$P_{34} = (1, 4, 3)$	$P_{51} = (1, 9, 7)$	$P_{68} = (1, 7, 1)$

$P_{69} = (1, 6, 8)$	$P_{86} = (1, 6, 7)$	$P_{103} = (1, 0, 9)$	$P_{120} = (1, 10, 0)$
$P_{70} = (1, 8, 1)$	$P_{87} = (1, 8, 9)$	$P_{104} = (1, 7, 10)$	$P_{121} = (1, 9, 10)$
$P_{71} = (1, 10, 2)$	$P_{88} = (1, 3, 9)$	$P_{105} = (1, 7, 5)$	$P_{122} = (1, 9, 5)$
$P_{72} = (1, 7, 0)$	$P_{89} = (1, 3, 8)$	$P_{106} = (1, 10, 3)$	$P_{123} = (0, 1, 7)$
$P_{73} = (1, 0, 7)$	$P_{90} = (1, 6, 9)$	$P_{107} = (1, 9, 2)$	$P_{124} = (1, 10, 1)$
$P_{74} = (1, 3, 10)$	$P_{91} = (0, 1, 8)$	$P_{108} = (1, 4, 2)$	$P_{125} = (1, 9, 1)$
$P_{75} = (1, 6, 10)$	$P_{92} = (1, 3, 7)$	$P_{109} = (1, 1, 3)$	$P_{126} = (1, 8, 4)$
$P_{76} = (1, 6, 5)$	$P_{93} = (1, 2, 3)$	$P_{110} = (1, 7, 9)$	$P_{127} = (0, 1, 2)$
$P_{77} = (1, 5, 4)$	$P_{94} = (1, 10, 6)$	$P_{111} = (1, 10, 5)$	$P_{128} = (1, 4, 0)$
$P_{78} = (1, 6, 4)$	$P_{95} = (1, 9, 6)$	$P_{112} = (1, 5, 8)$	$P_{129} = (0, 1, 4)$
$P_{79} = (1, 4, 1)$	$P_{96} = (1, 7, 4)$	$P_{113} = (1, 8, 0)$	$P_{130} = (0, 0, 1)$
$P_{80} = (1, 4, 9)$	$P_{97} = (1, 3, 4)$	$P_{114} = (1, 10, 8)$	$P_{131} = (0, 1, 10)$
$P_{81} = (1, 2, 6)$	$P_{98} = (1, 4, 6)$	$P_{115} = (1, 1, 7)$	$P_{132} = (1, 2, 0)$
$P_{82} = (1, 5, 9)$	$P_{99} = (1, 5, 6)$	$P_{116} = (0, 1, 9)$	$P_{133} = (0, 1, 0)$
$P_{83} = (0, 1, 3)$	$P_{100} = (1, 5, 1)$	$P_{117} = (1, 7, 2)$	
$P_{84} = (1, 8, 3)$	$P_{101} = (0, 1, 5)$	$P_{118} = (1, 8, 6)$	
$P_{85} = (1, 1, 9)$	$P_{102} = (1, 9, 0)$	$P_{119} = (1, 5, 0)$	

A.3 Distributed classification of arcs of degree five with GAP and the ScScP package

Files needed to submit jobs to run a pool of GAP ScScP servers on the cluster

1. `five_points.g` - a collection of GAP codes for sequential and parallel arcs classification. This file has the following content:

```

LoadPackage("fining");
LoadPackage("images");
LoadPackage("scscp");
SetInfoLevel( InfoFinInG, 0 );

pg := PG(2,11);
points := AsList(Points(pg));
lines := AsList(Lines(pg));
pgl := ProjectivityGroup(pg);
pgl_perm := Action(pgl, points, OnProjSubspaces);
perm_lines := List(lines, l -> Set(List(Points(l), p -> Position(points,
    ↪ p))));

Find5PointPerm := function(input)
    local elm, five_sec, remainder, stab, orbs,
        new, res, p, Comp_ones, RES;
    Comp_ones:=[]; RES:=[];
    res := Set([]);
    for elm in input do
        five_sec := Filtered(perm_lines, x -> Length(Intersection(elm,x)) =
            ↪ 5);
        remainder := Difference([1..Length(points)], Union(five_sec));
        remainder := Difference(remainder, elm);
        if Length(remainder) > 0 then
            stab := Stabilizer(pgl_perm, elm, OnSets);
            orbs := Orbits(stab, remainder);
            for p in orbs do
                # this looks like there's something wrong above

```

```

        AddSet(res, CanonicalImage(pgl_perm, Union(elm, [p[1]]),
        ↪ OnSets));
    od;
fi;
od;
return res;
end;

ParFind5PointPerm := function(input, chunksize)
local nr_inputs, tasks, r1, r2, RES, curtime1, curtime2;
nr_inputs:=Length(input);
tasks := [];
r1 := 1;
r2 := Minimum(chunksize, nr_inputs);
repeat
    Add( tasks, IO_PickleToString(input{[ r1 .. r2 ]}));
    r1 := r1 + chunksize;
    r2 := Minimum(r2+chunksize, nr_inputs);
until r1>nr_inputs;
curtime1:=IO_gettimeofday();
RES := Set( Concatenation( List( ParListWithSCSCP( tasks, "Find5PointPerm"
    ↪ ), IO_UnpickleFromString ) ) );
curtime2:=IO_gettimeofday();
return rec( arcs := RES[1], Comp_arcs := RES[2], time :=
    ↪ runtime(curtime1, curtime2));
end;

```

2. registry.g: is a configuration file for the registry GAP ScScP.
3. start_worker.sh: is a script to start one GAP ScScP server using the cluster job submission system.
4. submit_job.sh: is a script to submit an array job which will start a farm of GAP ScScP servers.

The files registry.g, start_worker.sh and submit_job.sh templates are exists with the same names in the ScScP package directory which resides in pkg directory of GAP. We just need to customise it depends on our needs.

Setting up

If you are starting a pool of GAP SCSCP servers automatically via the job submission system, you may need to edit options for the batch system in the beginning of `submit_job.sh` to specify your username, default queue and other details, and update the GAP directory path in `start_worker.sh`. After that, first need to start the registry server to which these servers will report their locations as soon as they will be about to start. You may run the registry server on a dedicated machine outside the cluster, or via an interactive job on the cluster. In both cases, start GAP and read the `registry.g` file. Then you will see the following message:

```
#I  Ready to accept TCP/IP connections at 0.0.0.0:26133 ...
```

Next, submit an array job to start a farm of GAP SCSCP servers by typing as follows:

```
qsub -t N1-N2 submit_job.sh start_worker.sh registryhostname
```

5. Now, when the pool of SCSCP servers should be running, you can start the GAP master with the command:

```
gap five_points.g.
```

When you are using the cluster with the registry server, you can simply retrieve the list of SCSCP servers from the registry:

```
SCSCPservers:=EvaluateBySCSCP( "KnownSCSCPservers", [], "registryhostname",  
  ↪ 26133 ).object;
```

6. Now you should be able to call `ParFind5PointPerm` which takes two arguments: the arcs list and the chunksize. For example, below we compute arcs of degree 5 and length 8 and 9:

```
gap> Length(perm_inp);  
8_5_arcs:=ParFind5PointPerm(perm_inp,5).arcs;;  
Length(8_5_arcs);  
10  
#I  1/2:master --> localhost:26133  
#I  2/2:master --> localhost:26134  
162  
gap> 9_5_arcs:=ParFind5PointPerm(8_5_arcs,10).arcs;;  
      Length(9_5_arcs);  
#I  1/17:master --> localhost:26133  
#I  2/17:master --> localhost:26134
```

```
#I 3/17:master --> localhost:26133
#I 4/17:master --> localhost:26134
#I 5/17:master --> localhost:26133
#I 6/17:master --> localhost:26134
#I 7/17:master --> localhost:26134
#I 8/17:master --> localhost:26133
#I 9/17:master --> localhost:26134
#I 10/17:master --> localhost:26133
#I 11/17:master --> localhost:26133
#I 12/17:master --> localhost:26134
#I 13/17:master --> localhost:26133
#I 14/17:master --> localhost:26134
#I 15/17:master --> localhost:26133
#I 16/17:master --> localhost:26134
#I 17/17:master --> localhost:26133
4404
```

Appendix B

Orbiter makefiles and labelling of points

B.1 Orbiter labelling of points in PG(2, 11)

More details can be found in [10] about Orbiter installation and the commands used in this appendix.

$P_1 = (1, 0, 0)$	$P_{18} = (1, 0, 3)$	$P_{35} = (0, 1, 6)$	$P_{52} = (1, 6, 2)$
$P_2 = (0, 1, 0)$	$P_{19} = (1, 0, 9)$	$P_{36} = (1, 2, 1)$	$P_{53} = (1, 2, 8)$
$P_3 = (0, 0, 1)$	$P_{20} = (1, 0, 2)$	$P_{37} = (1, 1, 6)$	$P_{54} = (1, 10, 7)$
$P_4 = (1, 1, 1)$	$P_{21} = (1, 0, 8)$	$P_{38} = (1, 8, 4)$	$P_{55} = (1, 4, 5)$
$P_5 = (1, 1, 0)$	$P_{22} = (1, 0, 7)$	$P_{39} = (1, 6, 3)$	$P_{56} = (1, 8, 10)$
$P_6 = (1, 6, 0)$	$P_{23} = (1, 0, 5)$	$P_{40} = (1, 7, 9)$	$P_{57} = (0, 1, 3)$
$P_7 = (1, 4, 0)$	$P_{24} = (1, 0, 10)$	$P_{41} = (1, 4, 2)$	$P_{58} = (1, 4, 1)$
$P_8 = (1, 3, 0)$	$P_{25} = (0, 1, 1)$	$P_{42} = (1, 5, 8)$	$P_{59} = (1, 2, 6)$
$P_9 = (1, 9, 0)$	$P_{26} = (1, 6, 6)$	$P_{43} = (1, 3, 7)$	$P_{60} = (1, 5, 4)$
$P_{10} = (1, 2, 0)$	$P_{27} = (1, 4, 4)$	$P_{44} = (1, 10, 5)$	$P_{61} = (1, 1, 3)$
$P_{11} = (1, 8, 0)$	$P_{28} = (1, 3, 3)$	$P_{45} = (1, 9, 10)$	$P_{62} = (1, 3, 9)$
$P_{12} = (1, 7, 0)$	$P_{29} = (1, 9, 9)$	$P_{46} = (0, 1, 4)$	$P_{63} = (1, 8, 2)$
$P_{13} = (1, 5, 0)$	$P_{30} = (1, 2, 2)$	$P_{47} = (1, 3, 1)$	$P_{64} = (1, 10, 8)$
$P_{14} = (1, 10, 0)$	$P_{31} = (1, 8, 8)$	$P_{48} = (1, 7, 6)$	$P_{65} = (1, 6, 7)$
$P_{15} = (1, 0, 1)$	$P_{32} = (1, 7, 7)$	$P_{49} = (1, 1, 4)$	$P_{66} = (1, 9, 5)$
$P_{16} = (1, 0, 6)$	$P_{33} = (1, 5, 5)$	$P_{50} = (1, 9, 3)$	$P_{67} = (1, 7, 10)$
$P_{17} = (1, 0, 4)$	$P_{34} = (1, 10, 10)$	$P_{51} = (1, 5, 9)$	$P_{68} = (0, 1, 9)$

$P_{69} = (1, 5, 1)$	$P_{86} = (1, 4, 8)$	$P_{103} = (1, 4, 6)$	$P_{120} = (1, 8, 7)$
$P_{70} = (1, 8, 6)$	$P_{87} = (1, 9, 7)$	$P_{104} = (1, 10, 4)$	$P_{121} = (1, 1, 5)$
$P_{71} = (1, 9, 4)$	$P_{88} = (1, 8, 5)$	$P_{105} = (1, 2, 3)$	$P_{122} = (1, 2, 10)$
$P_{72} = (1, 4, 3)$	$P_{89} = (1, 5, 10)$	$P_{106} = (1, 6, 9)$	$P_{123} = (0, 1, 10)$
$P_{73} = (1, 1, 9)$	$P_{90} = (0, 1, 8)$	$P_{107} = (1, 5, 2)$	$P_{124} = (1, 10, 1)$
$P_{74} = (1, 10, 2)$	$P_{91} = (1, 7, 1)$	$P_{108} = (1, 9, 8)$	$P_{125} = (1, 5, 6)$
$P_{75} = (1, 7, 8)$	$P_{92} = (1, 9, 6)$	$P_{109} = (1, 1, 7)$	$P_{126} = (1, 7, 4)$
$P_{76} = (1, 2, 7)$	$P_{93} = (1, 6, 4)$	$P_{110} = (1, 7, 5)$	$P_{127} = (1, 8, 3)$
$P_{77} = (1, 3, 5)$	$P_{94} = (1, 10, 3)$	$P_{111} = (1, 3, 10)$	$P_{128} = (1, 2, 9)$
$P_{78} = (1, 6, 10)$	$P_{95} = (1, 8, 9)$	$P_{112} = (0, 1, 5)$	$P_{129} = (1, 9, 2)$
$P_{79} = (0, 1, 2)$	$P_{96} = (1, 3, 2)$	$P_{113} = (1, 9, 1)$	$P_{130} = (1, 3, 8)$
$P_{80} = (1, 6, 1)$	$P_{97} = (1, 1, 8)$	$P_{114} = (1, 10, 6)$	$P_{131} = (1, 4, 7)$
$P_{81} = (1, 3, 6)$	$P_{98} = (1, 5, 7)$	$P_{115} = (1, 3, 4)$	$P_{132} = (1, 6, 5)$
$P_{82} = (1, 2, 4)$	$P_{99} = (1, 2, 5)$	$P_{116} = (1, 5, 3)$	$P_{133} = (1, 1, 10)$
$P_{83} = (1, 7, 3)$	$P_{100} = (1, 4, 10)$	$P_{117} = (1, 4, 9)$	
$P_{84} = (1, 10, 9)$	$P_{101} = (0, 1, 7)$	$P_{118} = (1, 7, 2)$	
$P_{85} = (1, 1, 2)$	$P_{102} = (1, 8, 1)$	$P_{119} = (1, 6, 8)$	

B.2 Large arcs and blocking sets

```

MY_PATH=~/Desktop/orbiter \\Here is where Orbiter lives
ORBITER=$(MY_PATH)/ORBITER
SRC=$(ORBITER)/src
ARCS_PATH=$(SRC)/apps/arcs
TOOLS_PATH=$(SRC)/apps/tools
PROJECTIVE_SPACE_PATH=$(SRC)/apps/projective_space
GROUPS_PATH=$(SRC)/apps/groups
SOLVER_PATH=$(SRC)/apps/solver
LINEAR_SPACES_PATH=$(SRC)/apps/linear_spaces
GRAPH_THEORY_PATH=\$(SRC)/apps/graph_theory

```

The "cheat_PG2_11" command is used to create a "cheat sheet" of PG(2, 11) that is, a pdf file "PG_2_11.pdf" which has the indices for points and lines that Orbiter use as in Appendix B.1.

```

cheat_PG2_11:
$(PROJECTIVE_SPACE_PATH)/cheat_sheet_PG.out -n 2 -q 11
pdflatex PG_2_11.tex

```

```
open PG_2_11.pdf
```

To get the classification of arcs of degree 3 in $\text{PG}(2, 11)$ we issue the "classify_21_3_pg_2_11" command as follows:

```
classify_21_3_pg_2_11:
    -mkdir arcs_21_3
$(ARCS_PATH)/arcs_main.out -v 5 -q 11 -d 3 -n 2 \
-input_prefix ./arcs_21_3/ \
-output_prefix ./systems/ \
-solution_prefix ./solutions/ \
-base_fname arcs_21_3
```

To implement the method explained in Section 6.5 we use the command "simeon" which gives a file called "solutions.txt" that has the $(77, 8)$ -arcs.

```
simeon:
$(PROJECTIVE_SPACE_PATH)/simeon.out -v 2
```

A call to the "simeon_iso" command would invoke Orbiter to classify the $(77, 8)$ -arcs in the "solutions.txt" file. Then a new file is created with the 134 isomorphism types of $(77, 8)$ -arcs in $\text{PG}(2, 11)$.

```
simeon_iso:
$(PROJECTIVE_SPACE_PATH)/canonical_form.out -v 2 -n 2 -q 11 \
-input \
-file_of_lines arc_lifting_simeon_q11_n2_d2_k5_solutions.txt \
-end \
-classify_nauty \
-prefix simeon_77_8_arcs \
-save simeon_77_8_arcs \
-latex
pdflatex simeon_77_8_arcs_classes.tex
open simeon_77_8_arcs_classes.pdf
```


Bibliography

- [1] A. Al-ogaidi and A. Betten. Large arcs in small planes. To appear in *Congressus Numerantium* journal. 2020.
- [2] S. Alabdullah and J. W. P. Hirschfeld. A new lower bound for the smallest complete (k, n) -arc in $\text{PG}(2, q)$. *Des. Codes Cryptogr.*, 87(2-3):679–683, 2019.
- [3] S. Ball. Multiple blocking sets and arcs in finite planes. *J. London Math. Soc. (2)*, 54(3):581–593, 1996.
- [4] S. Ball. *Finite Geometry and Combinatorial Applications*, volume 82 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2015.
- [5] S. Ball and J.W.P. Hirschfeld. Bounds on (n, r) -arcs and their application to linear codes. *Finite Fields Appl.*, 11(3):326–336, 2005.
- [6] J. Bamberg, A. Betten, J. De Beule, P. Cara, M. Lavrauw, and M. Neunhoeffler. FinInG - GAP package version 1.4.1, 2018.
- [7] A. Betten. Poset classification and optimal linear codes. *Submitted*.
- [8] A. Betten. Rainbow cliques and the classification of small BLT-sets. In *ISSAC 2013—Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, pages 53–60. ACM, New York, 2013.
- [9] A. Betten. The packings of $\text{PG}(3,3)$. *Des. Codes Cryptogr.*, 79(3):583–595, 2016.
- [10] A. Betten. Orbiter - A program to classify combinatorial objects, 2020.
- [11] R.C. Bose. Mathematical theory of the symmetrical factorial design. *Sankhya*, 8:107–166, 1947.
- [12] W. Cherowitzo. Bill Cherowitzo’s Hyperoval Page, 2019.
- [13] G. Cook. *Arcs in a finite projective plane*. PhD thesis, University of Sussex, 2011.
- [14] K. Coolsaet and H. Sticker. A full classification of the complete k -arcs of $\text{PG}(2,23)$ and $\text{PG}(2,25)$. *J. of Combin. Des.*, 17(6):459–477, 11 2009.

- [15] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.
- [16] W. Fulton. *Algebraic curves: an introduction to algebraic geometry*. Addison-Wesley, 1989.
- [17] B. Grünbaum. *Configurations of Points and Lines*. American Mathematical Soc.2009.
- [18] M. Hall. Ovals in the Desarguesian plane of order 16. *Ann. Mat. Pura Appl. (4)*, 102:159–176, 1975.
- [19] H. Hasse. Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung. *J. Reine Angew. Math.*, 175:193–208, 1936.
- [20] R. Hill. Some problems concerning (k, n) -arcs in finite projective planes. *Rend. Sem. Mat. Brescia*, 7:367–383, 1984.
- [21] R. Hill and C. Love. On the $(22,4)$ -arcs in $PG(2,7)$ and related codes. *Discrete Math.*, 266(1-3):253–261, 2003.
- [22] J. W. P. Hirschfeld. *Projective geometries over finite fields*. Clarendon Press, 1998.
- [23] J. W. P. Hirschfeld and E. V. D. Pichanick. Bounds for arcs of arbitrary degree in finite Desarguesian planes. *Journal of Combinatorial Designs*, 24(4):184–196, 2016.
- [24] C. Jefferson, E. Jonauskyte, M. Pfeiffer, and R. Waldecker. Minimal and canonical images. *Journal of Algebra*, 521:481–506, 2017.
- [25] C. Jefferson, M. Pfeiffer, R. Waldecker, and E. Jonauskyte. Images - GAP package version 1.3.0, 2019.
- [26] A Konovalov and S Linton. SCSCP–Symbolic Computation Software Composability Protocol, Version 1.2, 2010. GAP package.
- [27] S. Marcugini, A. Milani, and F. Pambianco. Classification of the $[n,3,n-3]_q$ NMDS codes over $GF(7)$, $GF(8)$ and $GF(9)$. *Ars Combin.*, 61:263–269, 2001.
- [28] S. Marcugini, A. Milani, and F. Pambianco. Maximal $(n,3)$ -arcs in $PG(2,13)$. *Discrete Math.*, 294(1-2):139–145, 2005.
- [29] B. McKay. Nauty User’s guide, Australian National University. *Computer Science Technical Report TR-CS-84-05*, 1984.
- [30] B. McKay. Isomorph-free exhaustive generation. *J. Algorithms*, 26(2):306–324, 1998.
- [31] J. Rose. *A course on group theory*. Courier Corporation, 1994.

- [32] B. Schmalz. Verwendung von Untergruppenleitern zur Bestimmung von Doppelnebenklassen. *Bayreuth. Math. Schr.*, (31):109–143, 1990.
- [33] B. Segre. Ovals in a finite projective plane. *Canad. J. Math.*, 7:414–416, 1955.
- [34] M. Soomro. *Algebraic curves over finite fields*. PhD thesis, University of Groningen, 2013.
- [35] The GAP group. GAP - Groups, Algorithms, and Programming, Version 4.10.2. <https://www.gap-system.org>, 2019.
- [36] G. Van Der Geer, E. Howe, K. Lauter, and C. Ritzenthaler. Manypoints: A table of curves with many points. *Online webpage: <http://www.manypoints.org>*, 2011.
- [37] M. Yazdi. *The classification of $(k; 3)$ -arcs over the Galois field of order five*. PhD thesis, University of Sussex, 1983.